



भारत का राजपत्र

The Gazette of India

असाधारण

EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)

PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं. 533]

नई दिल्ली, मंगलवार, अक्टूबर 17, 2000/आश्विन 25, 1922

No. 533]

NEW DELHI, TUESDAY, OCTOBER 17, 2000/ASVINA 25, 1922

सूचना प्रौद्योगिकी मंत्रालय

अधिसूचना

नई दिल्ली, 17 अक्टूबर, 2000

स.का.नि. 788(अ).—केंद्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 1 की उपधारा (3) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, तारीख 17 अक्टूबर, 2000 को उस तारीख के रूप में नियत करती है जिस तारीख को उक्त अधिनियम के उपबंध प्रवृत्त होंगे।

[सं. 1(20)/97-II डी (एन II)/एफ 6(i)]

पी. एम. सिंह, संयुक्त सचिव

MINISTRY OF INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 17th October, 2000

G.S.R. 788(E).—In exercise of the powers conferred by sub-section (3) of section 1 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby appoints 17th day of October, 2000 as the date on which the provisions of the said Act comes into force

[No. 1(20)/97-II (NII)/F 6(i)]

P. M. SINGH, Jt. Secy.

अधिसूचना

नई दिल्ली, 17 अक्टूबर, 2000

सा.का.नि. 789(अ)।— केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए प्रमाणकर्ता प्राधिकारियों के उपयोजन और अन्य मार्गदर्शक सिद्धांतों के विनियमन के लिए निम्नलिखित नियम बनाती है, अर्थात् :—

1. संक्षिप्त नाम और प्रारम्भ—(1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) नियम, 2000 है।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे।

2. परिमाण—इन नियमों में, जब तक संदर्भ से अन्यथा अपेक्षित न हों, —

(क) “अधिनियम” से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) “आवेदक” से प्रमाणकर्ता प्राधिकारी आवेदक अभिप्रेत है;

(ग) “संपरीक्षक” से ऐसा अन्तरराष्ट्रीय रूप से प्रत्यायित कम्प्यूटर सुरक्षा वृत्तिक या अभिकरण अभिप्रेत है जो प्रमाणकर्ता प्राधिकारी द्वारा नियुक्त और प्रमाणकर्ता प्राधिकारी के प्रचालनों की तकनीकी संपरीक्षा करने के लिए नियन्त्रक द्वारा मान्यताप्राप्त हो;

(घ) “नियंत्रक” से अधिनियम की धारा 17 की उपधारा (1) के अधीन नियुक्त प्रमाणकर्ता प्राधिकारियों का नियन्त्रक अभिप्रेत है;

(ड) “अंकीय चिह्नक प्रमाणपत्र” से अधिनियम की धारा 35 की उपधारा (4) के अधीन जारी किया गया अंकीय चिह्नक प्रमाणपत्र अभिप्रेत है;

(च) “सूचना आस्ति” से किसी संगठन के कारबार के अनुक्रम में प्रयुक्त सभी सूचना स्रोत अभिप्रेत हैं और इसके अंतर्गत सभी सूचना, उपयोजन (विकसित या क्रय किए गए साफ्टवेयर) और प्रौद्योगिकी (हार्डवेयर, सिस्टम साफ्टवेयर और नेटवर्क) हैं;

(छ) “अनुज्ञाप्ति” से इन नियमों के अधीन अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए किसी प्रमाणकर्ता प्राधिकारी को मंजूर की गई अनुज्ञाप्ति अभिप्रेत है;

(ज) “अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी” से ऐसा प्रमाणकर्ता प्राधिकारी अभिप्रेत है जिसे अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए अनुज्ञाप्ति प्रदान की गई है;

(झ) “व्यक्ति” के अंतर्गत कोई व्यष्टि या कोई कंपनी या व्यष्टियों का कोई संगम या निकाय, चाहे निर्गमित हो या न हो, या केन्द्रीय सरकार या कोई राज्य सरकार या ऐसी सरकारों का कोई मंत्रालय या विभाग, अभिकरण या प्राधिकारी आते हैं;

(ज) “अनुसूची” से इन नियमों से उपाबद्ध कोई अनुसूची अभिप्रेत है;

(ट) “हस्ताक्षरकर्ता पहचान सत्यापन शीति” से किसी अभिदाता की पहचान के सत्यापन और अधिप्रमाणन के लिए प्रयुक्त शीति अभिप्रेत है;

(ठ) “विश्वस्त व्यक्ति” से कोई ऐसा व्यक्ति अभिप्रेत है जो –

(i) उन कारोबारी क्रियाकलापों के दिन-प्रतिदिन के प्रचालनों, सुरक्षा और निष्पादन के लिए प्रत्यक्ष रूप से उत्तरदायी हो, जो प्रमाणकर्ता प्राधिकारी की बाबत अधिनियम या इन नियमों के अधीन विनियमित किए जाते हैं ; या

(ii) अंकीय चिह्नक प्रमाणपत्रों के जारी करने, नवीकरण, निलंबन या प्रतिसंहरण, (इसके अन्तर्गत किसी अनुज्ञाप्रमाणकर्ता प्राधिकारी से अंकीय चिह्नक प्रमाणपत्र का अनुरोध करने वाले किसी व्यक्ति की पहचान भी है), प्राइवेट कुंजियों के सूजन या प्रमाणकर्ता प्राधिकारियों की, अभिकलन प्रसुविधाओं के प्रशासन के संबंध में, कर्तव्यों से भारित किया गया हो ।

(ड) उन शब्दों और पदों के, जो इनमें प्रयुक्त हैं और परिभाषित नहीं हैं किन्तु अनुसूची-4 में परिभाषित हैं, वही अर्थ होंगे जो उस अनुसूची में हैं ।

3. वह रीति जिसमें सूचना अंकीय चिह्नक द्वारा अधिप्रमाणित की जाएगी-अंकीय चिह्नक,-

(क) का सूजन और सत्यापन, गूढ़लेखन द्वारा किया जाएगा जो स्वमेव कल्पित अबोध्य रूप में इलेक्ट्रॉनिक अभिलेख में बदलने और वापस लाने से संबंधित है ;

(ख) का ऐसा उपयोग किया जाएगा जिसे “लोक कुंजी गूढ़लेखन” के रूप में जाना जाता है, जिसमें दो विभिन्न अंकगणित संबंधित “कुंजियों” का-एक का अंकीय चिह्नक का सूजन या कल्पित अबोध्य रूप में डाटा के रूपांतरण के लिए और दूसरा कुंजी का अंकीय चिह्नक का सत्यापन के लिए या इलेक्ट्रॉनिक अभिलेख को मूल रूप में वापस लाने के लिए उपयोग करके,

द्रुतान्वेषण फलन के रूप में अभिहित प्रक्रिया का अंकीय चिह्नक के सूजन और सत्यापन, दोनों, में उपयोग किया जाएगा ।

स्पष्टीकरण : ऐसी दोनों कुंजियों का उपयोग करने वाले कम्प्यूटर उपकरण और साफ्टवेयर उपस्कर को प्रायः “असमिति गूढ़लेखन प्रणाली” के रूप में जाना जाता है ।

4. अंकीय चिह्नक का सूजन- किसी इलेक्ट्रॉनिक अभिलेख या सूचना के किसी अन्य मद पर चिह्न करने के लिए चिह्नकर्ता, पहले चिह्नकर्ता के साफ्टवेयर में द्रुतान्वेषण फलन का उपयोजन करेगा ; द्रुतान्वेषण फलन मानक लम्बाई के द्रुतान्वेषण परिणाम का अभिकलन करेगा जो इलेक्ट्रॉनिक अभिलेख के लिए अद्वितीय है (सभी व्यावहारिक प्रयोजनों के लिए); चिह्नकर्ता का साफ्टवेयर चिह्नकर्ता की प्राइवेट कुंजी का उपयोग करके द्रुतान्वेषण परिणाम को अंकीय चिह्नक में बदल देगा ; इलेक्ट्रॉनिक अभिलेख और उसे सृजित करने में प्रयुक्त प्राइवेट कुंजी दोनों के लिए अद्वितीय होंगे और अंकीय चिह्नक के साथ इलेक्ट्रॉनिक अभिलेख होगा तथा उसके इलेक्ट्रॉनिक अभिलेख के साथ भंडारित या पारेषित किया जाएगा ।

5. अंकीय चिह्नक का सत्यापन-अंकीय चिह्नक का सत्यापन मूल इलेक्ट्रॉनिक अभिलेख के नए द्रुतान्वेषण परिणाम के अभिकलन द्वारा अंकीय चिह्नक का सूजन करने के लिए प्रयुक्त उसी द्रुतान्वेषण फलन के माध्यम द्वारा और सत्यापन करने वाली लोक कुंजी और नए द्रुतान्वेषण परिणाम का उपयोग करके पूरा किया जाएगा, सत्यापक जांच करेगा तभी—

(i) यदि अंकीय चिह्नक का सूजन तत्संबंधी प्राइवेट कुंजी का उपयोग करके किया गया था ; और

(ii) यदि नया अभिकलित द्रुतान्वेषण परिणाम उस मूल परिणाम से मिलता जुलता है जो चिह्नाकान की प्रक्रिया के दौरान अंकीय चिह्नाकान में रूपांतरित किया गया था । सत्यापन साफ्टवेयर अंकीय चिह्नक की सत्यापित के रूप में पुष्टि करेगा, यदि -

(क) चिह्नकर्ता की प्राइवेट कुंजी इलेक्ट्रॉनिक अभिलेख के अंकीय चिह्न के लिए प्रयोग की गई थी, जिसे उस मामले के रूप में जाना जाता है यदि चिह्नकर्ता की लोक कुंजी चिह्नक के सत्यापन के

लिए प्रयोग की गई हो, क्योंकि चिह्नकर्ता की लोक कुंजी केवल चिह्नकर्ता की प्राइवेट कुंजी से सृजित अंकीय चिह्नक का ही सत्यापन करेगी ; और

(ख) इलेक्ट्रॉनिक अभिलेख अपरिवर्तित था, जिसे उस मामले के रूप में जाना जाता है यदि सत्यापक द्वारा अभिकलित द्रुतान्वेषण परिणाम सत्यापन प्रक्रिया के दौरान अंकीय चिह्नक से प्राप्त द्रुतान्वेषण परिणामों के समान है ।

6. मानक-प्रमाणकर्ता प्राधिकारियों के लिए सूचना प्रौद्योगिकी (आईटी) संरचना खुले मानकों और स्वीकृत वास्तविक मानकों का समर्थन करेगी ; अति महत्वपूर्ण मानक, जिन पर प्रमाणकर्ता प्राधिकारियों के कृत्यों से सहबद्ध विभिन्न क्रियाकलापों पर विचार किया जा सकेगा, निम्न प्रकार है :—

उत्पाद	मानक
लोक कुंजी अधोसंरचना	पी के आई एक्स
अंकीय चिह्नक प्रमाणपत्र और अंकीय चिह्नक प्रमाणपत्र प्रतिसंहरण सूची	एक्स. 509, आई टी यू आर एफ सी # 1422 में यथाविनिर्दिष्ट रूपांतर 3 प्रमाणपत्र
निदेशिका (डी ए पी और एल. डी ए पी)	एक्स. 500 प्रमाणपत्रों और प्रमाणन प्रतिसंहरण सूचियों (सी आर एलएस) के प्रकाशन के लिए
आंकड़ा संचय प्रबंधन संक्रियाएं	जेनेरिक एस क्यू एल का प्रयोग
लोक कुंजी एलोरिथ्म	डी एस ए और आर एस ए
अंकीय द्रुतान्वेषण फलन	एम डी 5 और एस एच ए - 1
आर एस ए लोक कुंजी प्रौद्योगिकी	पी के सी एस # 1 आर एस ए गूडलेखन मानक (512, 1024, 2048 बिट)
	पी के सी एस # 5 पारण शब्द आधारित गूडलेखन मानक
	पी के सी एस # 7 गूडलेखी संदेश वाक्य रचना मानक
	पी के सी एस # 8 प्राइवेट कुंजी सूचना वाक्य रचना मानक
	पी के सी एस # 9 चयनित प्रतीक प्ररूप
	पी के सी एस # 10 प्रमाणीकरण अनुरोध
	पी के सी एस # 12 उपयोक्ता की प्राइवेट कुंजी और प्रमाणपत्रों के भंडारकरण/परिवहन के लिए सुबाह्य प्ररूप
सुभिन्न नाम	एक्स. 520
अंकीय गूडलेखन और अंकीय चिह्नक	पी के सी एस # 7
अंकीय चिह्नक अनुरोध प्ररूप	पी के सी एस # 10

7. अंकीय चिह्नकर्ता प्रमाणपत्र मानक— प्रमाणकर्ता प्राधिकारियों द्वारा जारी किए गए सभी अंकीय चिह्नक प्रमाणपत्र नियम 6 के अनुसार, आई टी यू एक्स. 509 रूपांतर 3 मानक के अनुसूच होंगे और उनमें अन्य बातों के साथ निम्नलिखित डाटा अंतर्विष्ट होंगा :

- (क) क्रम संख्यांक (प्रमाणकर्ता प्राधिकारी द्वारा अंकीय चिह्नक प्रमाणपत्र को उसे अन्य प्रमाणपत्र से सुभिन्न करने के लिए क्रम संख्यांक देना) ;
- (ख) चिह्नक एल्गोरिद्म अभिज्ञापक (जो अंकीय चिह्नक प्रमाणपत्र पर चिह्न करने के लिए प्रमाणकर्ता प्राधिकारी द्वारा प्रयोग की गई एल्गोरिद्म का अभिज्ञान करता है) ;
- (ग) जारीकर्ता का नाम (उस प्रमाणकर्ता प्राधिकारी का नाम जिसने अंकीय चिह्नक प्रमाण जारी किया है) ;
- (घ) अंकीय चिह्नक प्रमाणपत्र की विधिमान्यता अवधि ;
- (ङ) हस्ताक्षरकर्ता का नाम (प्रमाणपत्र जिसकी लोक कुंजी का अभिज्ञान करता है) ; और
- (च) हस्ताक्षरकर्ता की लोक कुंजी सूचना ।

8. प्रमाणकर्ता प्राधिकारियों का अनुज्ञापन—(1) निम्नलिखित व्यक्ति, अंकीय चिह्नक प्रमाणपत्र जारी करने की अनुज्ञाप्ति के लिए आवेदन कर सकते हैं, अर्थात् :—

- (क) कोई व्यक्ति जो भारत का नागरिक हो और जिसके पास उसके कारबाह या वृत्ति में पांच करोड़ रुपए या अधिक की पूँजी हो;
- (ख) कोई कंपनी, जिसके पास—
 - (i) संदत्त पूँजी पांच करोड़ रुपए अन्यून हो ; और
 - (ii) शुद्ध धन पचास करोड़ रुपए से अन्यून हो :

परन्तु ऐसी कोई कंपनी जिसकी सकल रूप से उसकी शेयरपूँजी की उच्चास प्रतिशत से अधिक साधारण शेयरपूँजी अनिवासी भारतीयों, विदेशी संस्थागत निवेशकर्ताओं और विदेशी कंपनियों द्वारा धारण की जाती है, अनुज्ञाप्ति मंजूर किए जाने के लिए पात्र नहीं होगी :

परन्तु यह और कि जहां कंपनी की दशा में जिसने कंपनी अधिनियम, 1956 (1956 का 1) के अधीन रजिस्ट्रीकृत है पिछले वित्तीय वर्ष के दौरान या इस अधिनियम के अधीन अनुज्ञाप्ति के लिए वित्तीय वर्ष के दौरान अनुदत्त करने के लिए आवेदन किया है और जहां प्रमाणकर्ता प्राधिकारी को इस अधिनियम में के मुख्य उद्देश्य में इस खंड के उपखंड (ii) में निर्दिष्ट शुद्ध धन, हिन्दू अविभक्त कुटुम्ब फर्म या कंपनी की दशा में संदत्त साधारण पूँजी का कम से कम 51% धारण करने वाले उसके बहुमत शेयर धारकों का सकल शुद्ध धन होगा :

परन्तु यह भी कि दूसरे परन्तुक में निर्दिष्ट बहुमत शेयर धारकों में अनिवासी भारतीय, विदेशी राष्ट्रीय, विदेशी संस्थागत निवेशकर्ता और विदेशी कंपनी सम्मिलित नहीं होंगे :

परन्तु यह भी कि दूसरे परन्तुक में निर्दिष्ट कंपनी के बहुमत शेयर धारक, जिनका शुद्ध धन बहुमत शेयर धारकों के आधार पर अवधारित किया गया है, ऐसी कंपनी में धृत अपने साधारण शेयरों का विक्रय या अंतरण तब तक नहीं करेंगे जब तक कि,—

- (i) ऐसी कंपनी पचास करोड़ रुपए से अन्यून अर्जित नहीं कर लेती है या उसका अपना शुद्ध धन इतना नहीं हो जाता है ;
- (ii) नियंत्रक का पूर्वानुमोदन नहीं प्राप्त कर लेती है ;

(ग) कोई फर्म, जिसके—

- (i) सभी भागीदारों द्वारा प्रतिश्रुत पूंजी पांच करोड़ रुपए से कम नहीं है ;
- (ii) और शुद्ध धन पचास करोड़ रुपए से कम नहीं है :

परन्तु ऐसी कोई फर्म जिसमें किसी अनिवासी भारतीय और विदेशी राष्ट्रिक द्वारा धृत सकल पूंजी उसकी पूंजी के उच्चास प्रतिशत से अधिक है, अनुज्ञाति प्रदान करने के लिए पात्र नहीं होगी :

परन्तु यह और कि ऐसे मामले में जहां फर्म पूर्ववर्ती वित्तीय वर्ष के दौरान या उस वित्तीय वर्ष में जिसमें वह अधिनियम के अधीन अनुज्ञाति प्रदान करने के लिए आवेदन करती है भारतीय भागीदारी अधिनियम, 1932 (1932 का 9) के अधीन रजिस्टर की गई है और जिसका मुख्य उद्देश्य प्रमाणकर्ता प्राधिकारी के रूप में कृत्य करना है, इस खंड के उपखंड (ii) में निर्दिष्ट शुद्ध धन उसके सभी भागीदारों का सकल शुद्ध धन होगा :

परन्तु यह भी कि दूसरे परन्तुक में निर्दिष्ट भागीदारों में अनिवासी भारतीय और विदेशी राष्ट्रिक सम्मिलित नहीं होंगे :

परन्तु यह भी कि दूसरे परन्तुक में निर्दिष्ट किसी फर्म के ऐसे भागीदार जिसका शुद्ध धन ऐसे भागीदारों के आधार पर अवधारित किया गया है, ऐसी फर्म में उनके द्वारा धृत अपनी पूंजी का तब तक विक्रय या अंतरण नहीं करेगा जब तक कि—

- (i) सभी भागीदारों द्वारा प्रतिश्रुत पूंजी पांच करोड़ रुपए से कम नहीं है ;
- (ii) और शुद्ध धन पचास करोड़ रुपए से कम नहीं है ;

(घ) केन्द्रीय सरकार या कोई राज्य सरकार या ऐसी सरकारों का कोई मंत्रालय या विभाग या अभिकरण या प्राधिकारी ।

स्पष्टीकरण—इस नियम के प्रयोजन के लिए,—

(i) “कंपनी” का वही अर्थ होगा, जो आय-कर अधिनियम, 1961 (1961 का 43) की धारा 2 के खंड (17) में है ;

(ii) “फर्म”, “भागीदार” और “भागीदारों” के क्रमशः वहीं अर्थ होंगे जो उनके भारतीय भागीदारी अधिनियम, 1932 (1932 का 9) में हैं किन्तु “भागीदार” पद में ऐसा कोई व्यक्ति भी सम्मिलित होगा जिसे अवयस्क होने के कारण भागीदारी के फायदों में शामिल किया गया है ;

(iii) “विदेशी कंपनी” का वही अर्थ होगा जो उसका आय-कर अधिनियम, 1961 (1961 का 43) की धारा 2 के खंड (23क) में है ;

(iv) “शुद्ध धन” का वही अर्थ होगा, जो रूपण औद्योगिक कंपनी (विशेष उपबंध) अधिनियम, 1985 (1986 का 1) की धारा 3 की उपधारा (1) के खंड (छक) में है ;

(v) “अनिवासी” का वही अर्थ होगा, जो आय-कर अधिनियम, 1961 की धारा 2 के खंड (26) में है ;

(2) आवेदक, जो कोई व्यक्ति, उपनियम (1) के अधीन कोई कंपनी या कोई फर्म है, नियंत्रक के पक्ष में, नियंत्रक द्वारा अनुमोदित प्रस्तुति और रीति में, किसी अनुसूचित बैंक से ऐसी रकम का जो पांच करोड़ रुपए के कम न होगी, निष्पादन बंधपत्र या बैंकर प्रत्याभूति प्रस्तुत करेगा । निष्पादन बंधपत्र या बैंकर की प्रत्याभूति उसके प्रस्तुत किए जाने की तारीख से छह वर्ष की अवधि के लिए विधिमान्य रहेगी :

परन्तु खंड (ख) के दूसरे परन्तुक में और उपनियम (1) के खंड (ग) के दूसरे परन्तुक में निर्दिष्ट कंपनी और फर्म दस करोड़ रुपए का कार्य निष्पादन बंधपत्र देंगे या बैंकर की प्रत्याभूति प्रस्तुत करेंगे :

परन्तु यह और कि पहले परन्तुक की कोई भी बात कंपनी या फर्म को, उसके द्वारा पचास करोड़ रुपए का शुद्ध धन अर्जित कर लिए जाने या उसका अपना धन इतना हो जाने के पश्चात् लागू नहीं होगी ।

(3) ऐसी किसी शास्ति या अभियोजन पर, जो इस अधिनियम या तत्समय प्रवृत्त किसी अन्य विधि के अधीन अधिरोपित की जा सकेगी या प्रारंभ किया जा सकेगा, प्रतिकूल प्रभाव डाले बिना निष्पादन बंधपत्र या बैंकर प्रत्याभूति का निम्नलिखित के लिए अवलंब लिया जा सकेगा—

(क) जब नियंत्रक ने अधिनियम की धारा 25 की उपधारा (2) के अधीन अनुज्ञाप्ति का निलंबन कर दिया हो ; या

(ख) नियंत्रक द्वारा किए गए प्रतिकर के किसी प्रस्ताव के संदाय के लिए ; या

(ग) प्रमाणकर्ता प्राधिकारी, उसके अधिकारियों या कर्मचारियों की उपेक्षा के कारण हुए दायित्वों और परिशुद्धि खर्चों के संदाय के लिए ; या

(घ) अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के प्रचालनों को बंद करने या अंतरण में उपगत खर्चों के संदाय के लिए, यदि प्रमाणकर्ता प्राधिकारी की अनुज्ञाप्ति या प्रचालन बंद कर दिया जाता है ; या

(ङ) अधिनियम या तद्धीन बनाए गए नियमों के उपबंधों के अनुपालन में प्रमाणकर्ता प्राधिकारी द्वारा की गई कोई अन्य चूक ।

स्पष्टीकरण—“प्रचालन का अंतरण” का वही अर्थ होगा जो आय-कर अधिनियम, 1961 (1961 का 43) की धारा 2 के खंड (47) में दिया गया है ।

9. प्रसुविधाओं का स्थान-अंकीय चिह्नक प्रमाणपत्र के बनाए जाने, जारी किए जाने और प्रबंधन के सभी कृत्यों से सहबद्ध अधोसंरचना और अंकीय चिह्नक प्रमाणपत्र की प्रास्थिति और विधिमान्यता के बारे में सूचना रखने वाली निदेशिकाओं का अनुरक्षण भारत में किसी स्थान पर स्थापित किया जाएगा ।

10. आवेदन प्रस्तुत किया जाना-अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के लिए प्रत्येक आवेदन नियंत्रक को निम्नानुसार किया जाएगा,—

(i) अनुसूची 1 में दिए गए प्ररूप में ; और

(ii) ऐसी रीति से जो नियंत्रक द्वारा समय-समय पर अवधारित की जाए और वह ऐसे दस्तावेजों और सूचना से समर्थित होगा जिसकी नियंत्रक द्वारा अपेक्षा की जाए और इसमें अन्य बातों के साथ निम्नलिखित होंगे—

(क) प्रमाणीकरण पद्धति विवरण (सी पी एस);

(ख) कोई विवरण जिसके अंतर्गत आवेदक का अभिज्ञान करने की बाबत प्रक्रियाएं भी आती है ;

(ग) बाहर से प्राप्त की जाने वाली प्रत्याशित अंकीय चिह्नक प्रमाणपत्र प्रौद्योगिकी, प्रबंध या प्रचालनों का प्रयोजन और विस्तार का विवरण ;

(घ) प्रमाणकर्ता प्राधिकारी के कारबार रजिस्ट्रीकरण दस्तावेजों की प्रमाणित प्रतियां जो अनुज्ञाप्ति के लिए आशयित हैं ;

(ङ) ऐसी किसी घटना का विवरण, विशिष्टतया चालू या पिछला दिवालियापन, जो आवेदक की प्रमाणकर्ता प्राधिकारी के रूप में कार्य करने की योग्यता को सारवान रूप में प्रभावित कर सकती है ;

(च) आवेदक द्वारा ऐसा वचनबंध जिसका वह अपनी जानकारी और विश्वास के अनुसार प्रमाणीकरण पद्धति विवरण (सी पी एस) की अपेक्षाओं के साथ अनुपालन कर सकेगा और करेगा ;

(छ) यह वचनबंध कि प्रमाणकर्ता प्राधिकारी का प्रचालन तबतक प्रारंभ नहीं होगा जब तक कि उसके प्रचालन और अंकीय चिट्ठनक प्रमाणपत्र उत्पादन जारी किए जाने और प्रबंधन के कृत्यों के साथ सहबद्ध सुविधाओं का संपरीक्षकों द्वारा संपरीक्षा और नियम 20 के अनुसार नियंत्रक द्वारा अनुमोदन नहीं कर दिया जाता ;

(ज) प्रमाणकर्ता प्राधिकारी के रूप में प्रचालन के लिए अनुज्ञाप्ति मंजूर करने के लिए नियंत्रक द्वारा अपना अनुमोदन के उपदर्शित करने के एक मास के भीतर नियम 8 के उपनियम (2) अनुसार निष्पादन बंधपत्र या बैंकर की प्रत्याभूति को प्रस्तुत करने का वंचनबंध ;

(झ) नियंत्रक द्वारा अपेक्षित कोई अन्य सूचना ।

11. फीस-(1) अनुज्ञाप्ति मंजूर करने के लिए आवेदन के साथ नियंत्रक के नाम में निकाले गए बैंक ड्राफ्ट द्वारा या संदाय आदेश द्वारा संदेय पच्चीस हजार रुपए की अप्रतिदेय फीस होगी ।

(2) प्रमाणकर्ता प्राधिकारी की अनुज्ञाप्ति के नवीकरण के लिए नियंत्रक को प्रस्तुत प्रत्येक आवेदन के साथ नियंत्रक के नाम में निकाले गए बैंकड्राफ्ट द्वारा या संदाय आदेश द्वारा संदेय पांच हजार रुपए की अप्रतिदेय फीस होगी ।

(3) फीस या उसका भाग वापस नहीं होगा यदि विधिमान्यता अवधि के दौरान, अनुज्ञाप्ति का निलंबन या प्रतिसंहरण किया जाता है ।

12. प्रतिप्रमाणन-(1) अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के पास भारत के भीतर अन्य अनुज्ञाप्त प्रमाणकर्ता प्राधिकारियों के साथ प्रतिप्रमाणन के लिए इंतजाम होगा जो उनके प्रचालनों के प्रारंभ करने के पूर्व नियंत्रक को नियम 20 के अनुसार प्रस्तुत किया जाएगा :

परन्तु यदि प्रमाणकर्ता प्राधिकारियों के बीच या प्रमाणकर्ता प्राधिकारियों या प्रमाणकर्ता प्राधिकारी और हस्ताक्षरकर्ता के बीच किसी ऐसे इंतजाम के परिणामस्वरूप कोई विवाद उद्भूत होता है तो माध्यस्थम या समाधान के लिए नियंत्रक को निर्दिष्ट किया जाएगा ।

(2) अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी द्वारा विदेशी प्रमाणकर्ता प्राधिकारी के साथ प्रतिप्रमाणन इंतजाम के साथ आवेदन नियंत्रक को ऐसे प्ररूप में और ऐसी रीति से प्रस्तुत किया जाएगा जिसका अपबंध नियंत्रक द्वारा बनाए गए चरित्रियों में किया गया हो ; और अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी, तब तक प्रतिप्रमाणन प्रचालन प्रारंभ नहीं करेगा जब तक उसने नियंत्रक द्वारा अनुमोदित लिखित या अंकीय चिट्ठनक प्राप्त न कर लिया हो ।

13. अनुज्ञाप्ति की विधिमान्यता-(1) कोई अनुज्ञाप्ति उसके जारी किए जाने की तारीख से पांच वर्ष की अवधि के लिए विधिमान्य होगी ।

(2) अनुज्ञाप्ति हस्तांतरणीय नहीं होगी ।

14. अनुज्ञाप्ति का निलंबन-(1) नियंत्रक, अधिनियम की धारा 25 की उपधारा (2) में अंतर्विष्ट उपबंधों के अनुसार आदेश द्वारा अनुज्ञाप्ति निलंबित कर सकेगा ।

(2) नियम 8 के उपनियम (1) के खंड (क) से (ग) में निर्दिष्ट व्यक्तियों को मंजूर की गई अनुज्ञाप्ति तब निलंबित रहेगी जब ऐसे व्यक्ति द्वारा प्रस्तुत निष्पादन बंध-पत्र या दी गई बैंकर प्रत्याभूति का उस नियम के उपनियम (2) के अधीन अबलंब लिया जाता है ।

15. अनुज्ञाप्ति का नवीकरण-(1) नियम 8 से नियम 13 के उपबंध किसी अनुज्ञाप्ति के नवीकरण आवेदन को उसी प्रकार लागू होंगे जैसे वे अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के लिए किसी नए आवेदन को लागू होते हैं ।

(2) कोई प्रमाणकर्ता प्राधिकारी, अपनी अनुज्ञाप्ति के नवीकरण के लिए कोई आवेदन अनुज्ञाप्ति की विधिमान्यता की अवधि की समाप्ति की तारीख से कम से कम पेंतालीस दिवस पूर्व करेगा ।

(3) अनुज्ञाप्ति के नवीकरण के लिए आवेदन इलेक्ट्रॉनिक अभिलेख के प्रस्तुत में ऐसी अपेक्षाओं के अधीन करेगा, जिन्हें नियंत्रक ठीक समझे ।

16. अनुज्ञाप्ति जारी किया जाना-(1) नियंत्रक, आवेदन की प्राप्ति की तारीख से चार सप्ताह के भीतर आवेदन से संलग्न दस्तावेजों और ऐसे अन्य कारकों पर, जो ठीक समझे जाएं, जारी करने के पश्चात् अनुज्ञाप्ति या उसका नवीकरण मंजूर या आवेदन को नामंजूर कर सकेगा :

परन्तु आपवादिक परिस्थितियों में और ऐसे कारणों से जो लिपिबद्ध किए जाएंगे, चार सप्ताह की अवधि का, ऐसी अवधि के लिए जो सब मूलाकर आठ सप्ताह से अधिक नहीं होगी और जो नियंत्रक द्वारा ठीक समझी जाए, विस्तार किया जा सकेगा ।

(2) यदि अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के लिए आवेदन का अनुमोदन किया जाता है तो आवेदक—

(क) नियंत्रक को ऐसे अनुमोदन की तारीख से एक मास के भीतर नियम 8 के उपनियम (2) के अनुसार एक निष्पादन बंधपत्र प्रस्तुत करेगा या बैंकर प्रत्याभूति देगा ; और

(ख) नियंत्रक के साथ अनुज्ञाप्ति के निबंधनों और शर्तों तथा अधिनियम और उसके अधीन बनाए गए नियमों के उपबंधों की अनुपालना करने के लिए स्वयं को आबद्ध करते हुए एक करार का निष्पादन करेगा ।

17. अनुज्ञाप्ति से इंकार-नियंत्रक, अनुज्ञाप्ति मंजूर करने या नवीकरण करने से इंकार कर सकेगा, यदि—

(i) आवेदक ने उसके कारबार और किन्ही ऐसी परिस्थितियों, जो उसके कारबार संचालित करने की पद्धति को प्रभावित करती हो, जैसा कि नियंत्रक द्वारा अपेक्षा की जाए, नियंत्रक को न दी हो, से संबंधित ऐसी सूचना ; या

(ii) आवेदक परिसमापन करने या परिनिर्धारण करने के प्रक्रम में हो ; या

(iii) न्यायालय द्वारा आवेदक की बाबत कोई रिसीवर या कोई रिसीवर और प्रबंधक नियुक्त किया गया है ; या

(iv) आवेदक या कोई विश्वस्त व्यक्ति या तो भारत में या भारत से बाहर किसी ऐसे अपराध का सिद्धदोष ठहराया गया है, जिसके लिए दोषसिद्धि में यह निष्कर्ष अंतर्वलित है कि उसने कपटपूर्वक या बेर्इमानी का कार्य किया है या उसे अधिनियम या इन नियमों के अधीन किसी अपराध के लिए सिद्धदोष ठहराया गया है ; या

(v) नियंत्रक के निष्पादन बंधपत्र या बैंकर प्रत्याभूति का अवलंब लिया है ; या

(vi) प्रमाणकर्ता प्राधिकारी, प्रमाणीकरण पद्धति विवरण में विहित प्रक्रियाओं और व्यवहारों को भंग करता है या उनके पालन और अनुपालन में असफल रहता है ; या

(vii) प्रमाणकर्ता प्राधिकारी, नियम 31 के अनुसार संपरीक्षा कराने या विवरणियों के प्रस्तुत करने में असफल रहता है ; या

(viii) संपरीक्षा रिपोर्ट में सिफारिश की गई है कि प्रमाणकर्ता प्राधिकारी, प्रमाणकर्ता प्राधिकारी के प्रचालनों को चालू रखने योग्य नहीं है ; या

(ix) प्रमाणकर्ता प्राधिकारी, नियंत्रक के निवेशों की अनुपालना में असफल रहता है ।

18. शासी विधियां-प्रमाणकर्ता प्राधिकारी का प्रमाणीकरण पद्धति विवरण देश की विधियों द्वारा शासित होगा और उनकी अनुपालना करेगा ।

19. प्रमाणकर्ता प्राधिकारियों के लिए सुरक्षा मार्गदर्शक सिद्धांत—(1) प्रमाणकर्ता प्राधिकारी का, उसके प्रचालन में नियोजित सूचना और सूचना आस्तियों का उनके मूल्य, संवेदनशीलता और प्रचालन के महत्व के अनुसार वर्गीकरण, अवर्गीकरण, लेबलिंग, भंडारकरण, अभिगमन और नाशकरण पर विचार करते हुए, विश्वसनीयता और गोपनीयता और संरक्षण का पूर्ण उत्तरदायित्व होगा ।

(2) सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शक सिद्धांत और प्रमाणकर्ता प्राधिकारी की सेवा की विश्वसनीयता, गोपनीयता और उपलब्धता के संरक्षण को ध्यान में रखते हुए प्रमाणकर्ता प्राधिकारियों के लिए सुरक्षा मार्गदर्शक सिद्धांत क्रमशः अनुसूची 2 और अनुसूची 3 में दिए गए हैं ।

(3) प्रमाणकर्ता प्राधिकारी इन मार्गदर्शक सिद्धांतों की अनुपालना करते हुए प्रचालन के लिए अपनी सूचना प्रौद्योगिकी और सुरक्षा नीति तैयार करेगा और प्रचालन के जारी करने से पहले उसे नियंत्रक को प्रस्तुत करेगा :

परन्तु सूचना प्रौद्योगिकी और सुरक्षा नीति में प्रमाणकर्ता प्राधिकार द्वारा किया गया कोई परिवर्तन उसके द्वारा दो सप्ताह के भीतर नियंत्रक को प्रस्तुत किया जाएगा ।

20. अनुज्ञाप्त प्रमाणकर्ता प्राधिकारियों द्वारा प्रचालन का प्रारंभ—अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी, अंकीय चिह्नक के उत्पादन और जारी करने का अपना वाणिज्यिक प्रचालन निम्नलिखित के पश्चात् ही करेगा —

(क) उसने नियंत्रक को प्रमाणीकरण पद्धति विवरण के अंगीकरण की पुष्टि कर दी हो ;

(ख) उसने कुंजीयुग्म अर्थात् प्राइवेट और तत्संबंधी लोक कुंजी का उत्पादन और लोक कुंजी नियंत्रक को प्रस्तुत कर दी हो ;

(ग) अंकीय चिह्नक प्रमाणपत्र के उत्पादन जारी करने और प्रबंधन से सहबद्ध संस्थापित प्रसुविधाओं, संरचना और सभी कृत्यों का संपरीक्षण नियम 31 के अनुसार प्रत्यायित संपरीक्षक द्वारा कर दिया गया हो ; और

(घ) उसने भारत में अन्य अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी के साथ प्रति प्रमाणीकरण के इंतजाम नियंत्रक को प्रस्तुत कर दिया हो ।

21. प्रमाणकर्ता प्राधिकारी के रूप में कार्य करना बंद करने से पूर्व अपेक्षाएं—प्रमाणकर्ता प्राधिकारी के रूप में कार्य करना बंद करने से पहले कोई प्रमाणकर्ता प्राधिकारी,—

(क) नियंत्रक को प्रमाणकर्ता प्राधिकारी के रूप में कार्य करना बंद करने के अपने आशय की सूचना देगा :

परन्तु सूचना प्रमाणकर्ता प्राधिकारी के रूप में कार्य बंद करने के कम से कम नब्बे दिवस पहले या अनुज्ञाप्ति की समाप्ति की तारीख से नब्बे दिवस पहले दी जाएगी ;

(ख) यथास्थिति, अनुज्ञाप्ति के अवसान या प्रमाणकर्ता प्राधिकारी के रूप में कार्य करना बंद करने से साठ दिवस पूर्व ऐसे आशय का विज्ञापन, ऐसे दैनिक समाचार-पत्र या समाचार पत्रों में और ऐसी रीति से जो नियंत्रक अवधारित करे, करेगा ;

(ग) प्रमाणकर्ता प्राधिकारी के रूप में कार्य बंद करने के अपना आशय उसके द्वारा जारी किए गए प्रत्येक अप्रतिसंहित या अनवसित अंकीय चिह्नक प्रमाणपत्र के हस्ताक्षरकर्ता और प्रति प्रमाणीकरण प्राधिकारी को अधिसूचित करेगा :

परन्तु सूचना, यथास्थिति, प्रमाणकर्ता प्राधिकारी के रूप में कार्य बंद करने से कम से कम साठ दिवस पूर्व या अप्रतिसंहित या अनवसित अंकीय चिह्नक प्रमाणपत्र की समाप्ति की तारीख से कम से कम साठ दिवस पूर्व, दी जाएगी ।

(घ) सूचना नियंत्रक, प्रभावित हस्ताक्षरकर्ता और प्रति प्रमाणीकरण प्राधिकारी को अर्काय निःन्दा उन्मेल और रजिस्ट्रीकृत डाक द्वारा भेजी जाएगी ;

(ङ) ऐसे शेष अप्रतिसंहत या अनवसित सभी अंकीय चिह्नक प्रमाणपत्रों का प्रतिसंहरण नवे दिवस की सूचना अवधि की समाप्ति पर करेगा चाहे हस्ताक्षरकर्ता ने प्रतिसंहरण के लिए अनुरोध किया हो या न किया हो ;

(च) यह सुनिश्चित करने के युक्तियुक्त प्रयास करेगा कि उसकी प्रमाणीकरण सेवाओं के यद ऊरने से उसके हस्ताक्षरकर्ता और बकाया अंकीय चिह्नक प्रमाणपत्रों में अंतर्विष्ट लोक कुंजियों के निर्देश द्वारा अंतर्विष्ट लोक कुंजियों को सत्यापित करने के लिए सम्यक रूप से इच्छुक व्यक्तियों को न्यूनतम अवरोध कारित हो ।

(छ) अपने अभिलेखों के सात वर्ष की अवधि के लिए परिस्थिति के लिए युक्तियुक्त इंतजाम करे ।

(ज) हस्ताक्षरकर्ता को, उनके अवसान की तारीख से पहले उनके अंकीय चिह्नक प्रमाणपत्रों में, प्रतिसंहरण के लिए युक्तियुक्त प्रत्यास्थापन (नए अंकीय चिह्नक प्रमाणपत्र प्राप्त ऊरने में अतर्वलित अनुच्छेद अनधिक) का संदाय करे ।

(झ) प्रमाणकर्ता प्राधिकारी, अनुज्ञाप्ति में वर्णित अवसान की तारीख के पश्चात्, प्रमाणपत्र की अनुज्ञाप्ति कुंजी के नष्ट करने की तारीख और समय की पुष्टि करेगा ।

22. प्रमाणकर्ता प्राधिकारियों का डाटा संचय-नियन्त्रक, प्रत्येक प्रमाणकर्ता प्राधिकारी, प्रतिप्रमाणकर्ता प्राधिकारी और विदेशी प्रमाणकर्ता प्राधिकारी के प्रकटन अभिलेख का डाटा संचय बनाएगा जिसमें अन्य वातों के साथ निम्नलिखित व्योरे होगे ।

(क) व्यक्ति का नाम/निदेशकों के नाम, कारबाह की प्रकृति, आय-कर स्थाई लेखा सरकारी, वेब पता, यदि कोई है, कार्यालय और निवास का पता, अंकीय चिह्नक प्रमाणपत्र के उत्पादन के कृत्यों से सहबद्ध सुविधाओं का स्थान, वाक और प्रतिकृति टेलीफोन संख्या और इलेक्ट्रॉनिक डाक पता (पते), उसके प्रशासनिक संपर्क और उसका प्राधिकृत प्रतिनिधि ;

(ख) अंकीय चिह्नक प्रमाणपत्र पर अंकीय चिह्न करने के लिए प्रमाणकर्ता प्राधिकरी और मान्यताप्राप्त विदेशी प्रमाणकर्ता प्राधिकारी द्वारा प्रयुक्त प्राइवेट कुंजी (कुंजीओं) की तत्संबंधी लोक कुंजी (कुंजियों) ;

(ग) प्रमाणकर्ता प्राधिकारी के प्रमाणीकरण पद्धति विवरण के चालू और पिछले रूपांतर ;

(घ) निम्नलिखित की तारीख और समय उपदर्शित करते हुए समय मुद्राक—

(i) अनुज्ञाप्ति का जारी करना ,

(ii) प्रमाणकर्ता प्राधिकारी द्वारा प्रमाणीकरण पद्धति विवरण और उसके पूर्वतर रूपांतरों को अंगीकार करने की पुष्टि ,

(iii) प्रमाणकर्ता प्राधिकारी द्वारा अंकीय चिह्नक प्रमाणपत्र उत्पादन और जारी करने के वाणिज्यिक प्रचालनों का प्रारंभ ;

(iv) प्रमाणकर्ता प्राधिकारी की अनुज्ञाप्ति का प्रतिसंहरण या निलम्बन ;

(v) प्रतिप्रमाणकर्ता प्राधिकारी के प्रचालन का प्रारंभ ;

(vi) विदेशी प्रमाणकर्ता प्राधिकारी को मान्यता प्रदान करना ;

(vii) विदेशी प्रमाणकर्ता प्राधिकरी की मान्यता का प्रतिसंहरण या निलम्बन ।

23. अंकीय चिह्नक प्रमाणपत्र-प्रमाणकर्ता प्राधिकारी, अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए अधिनियम की धारा 35 के उपबंधों की अनुपालना करते समय निम्नलिखित की भी अनुपालना करेगा, अर्थात् :—

(क) अंकीय चिह्नक प्रमाणपत्र, हस्ताक्षरकर्ता द्वारा प्रमाणकर्ता प्राधिकारी द्वारा उपबंधित अंकीय चिह्नक प्रमाणपत्र आवेदन प्रस्तुत करने के पश्चात् और उसके अनुमोदन किए जाने के पश्चात् ही जारी किए जाएंगे :

परन्तु आवेदन प्रस्तुत में अन्य बातों के साथ अनुसूची 4 में दिए गए आदर्श प्रस्तुत में दी गई विशिष्टियां होगी ;

(ख) कोई अंतरिम अंकीय चिह्नक प्रमाणपत्र जारी नहीं किया जाएगा ;

(ग) अंकीय चिह्नक प्रमाणपत्र का निम्नलिखित के लिए प्राधिकृत और विधिमान्य अनुरोध की प्राप्ति पर प्रमाणकर्ता प्राधिकारी द्वारा उत्पादन किया जाएगा ;

(i) नया अंकीय चिह्नक प्रमाणपत्र ;

(ii) अंकीय चिह्नक प्रमाणपत्र नवीकरण ।

(घ) अंकीय चिह्नक प्रमाणपत्र में निर्देश द्वारा ऐसी सूचना अवश्य अंतर्विष्ट और समाहित होनी चाहिए, जो एक या अधिक निधानों का पता करने या पहचान करने के लिए पर्याप्त हो, जिसमें अंकीय चिह्नक प्रमाणपत्र के प्रतिसंहरण या निलम्बन सूचीबद्ध किया जाएगा, यदि अंकीय चिह्नक प्रमाणपत्र का निलम्बन या प्रतिसंहरण किया जाता है ;

(ड) अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए नियोजित अभिदाता पहचान सत्यापन रीति, प्रमाणीकरण पद्धति विवरण में विनिर्दिष्ट होनी चाहिए और यह अनुज्ञाप्ति के आवेदन के दौरान नियंत्रक के अनुमोदन के अधीन होगी ;

(च) जहां किसी व्यक्ति द्वारा धारित अन्य विधिमान्य अंकीय चिह्नक प्रमाणपत्र के आधार पर (जिसे इस खंड में मूल अंकीय चिह्नक प्रमाणपत्र कहा गया है) उसी व्यक्ति को अंकीय चिह्नक प्रमाणपत्र (जिसे इस खंड में नया अंकीय चिह्नक प्रमाणपत्र के रूप में निर्दिष्ट किया गया है) जारी किया जाता है और बाद में भूल अंकीय चिह्नक प्रमाणपत्र का निलम्बन या प्रतिसंहरण किया जाता है तो प्रमाणकर्ता प्राधिकारी, जिसने नया अंकीय चिह्नक प्रमाणपत्र जारी किया है, यह अवधारित कराने के लिए अनवेषण करेगा कि क्या नया अंकीय चिह्नक प्रमाणपत्र का निलम्बन या प्रतिसंहरण किया जाना आवश्यक है ;

(छ) प्रमाणकर्ता प्राधिकारी, हस्ताक्षरकर्ता को अंकीय चिह्नक प्रमाणपत्र को स्वीकार किए जाने से पहले उसकी अंतर्वस्तु के सत्यापन के लिए समुचित अवसर प्रदान करेगा ;

(ज) यदि हस्ताक्षरकर्ता जारी किए गए अंकीय चिह्नक प्रमाणपत्र को स्वीकार करता है तो प्रमाणकर्ता प्राधिकारी किसी निधान में अंकीय चिह्नक प्रमाणपत्र की चिह्नित प्रति प्रकाशित करेगा ;

(झ) जब अनुज्ञाप्त प्रमाणकर्ता प्राधिकारी द्वारा अंकीय चिह्नक प्रमाणपत्र जारी कर दिया गया हो और हस्ताक्षरकर्ता द्वारा स्वीकार कर लिया गया हो और प्रमाणकर्ता प्राधिकारी को, कोई ऐसा तथ्य ज्ञात हो, या अन्यथा, जो अंकीय चिह्नक प्रमाणपत्र की विधिमान्यता या विश्वसनीयता को सारभूत रूप से प्रभावित करता हो तो वह उसे हस्ताक्षरकर्ता को तुरन्त अधिसूचित करेगा ;

(ज) सभी अंकीय चिह्नक प्रमाणपत्र अभिहित अवसान तारीख के साथ जारी किए जाएंगे ।

24. अंकीय चिह्नक प्रमाणपत्र का उत्पादन—अंकीय चिह्नक प्रमाणपत्र के उत्पादन में निम्नलिखित अंतर्वलित है :

(क) अनुमोदित और सत्यापित अंकीय चिह्नक प्रमाणपत्र अनुरोध की प्राप्ति ;

(ख) नए अंकीय चिह्नक प्रमाणपत्र का सृजन ;

(ग) अंकीय चिह्नक प्रमाणपत्र स्वामी के अंकीय चिह्नक प्रमाणपत्र के साथ सहबद्ध कुंजी युग्मों की बाध्यता ;

(घ) प्रचालनात्मक उपयोग के लिए अंकीय चिह्नक प्रमाणपत्र और सहबद्ध लोक कुंजी का जारी किया जाना ;

(ङ) अंकीय चिह्नक प्रमाणपत्र स्वामी के साथ सहबद्ध कोई विशिष्ट नाम ; और

(च) प्रमाणीकरण पद्धति विवरण में यथापरिभाषित कोई मान्यता प्राप्त और सुसंगत नीति ।

25. अंकीय चिह्नक प्रमाणपत्र का जारी करना- प्रमाणकर्ता प्राधिकारी, अंकीय चिह्नक प्रमाणपत्र जारी करने से पहले :—

(i) यह पुष्टि करेगा कि प्रयोगकर्ता का नाम, उसकी जोखिम वाले प्रयोगकर्ताओं की सूची में नहीं है ;

(ii) उसके प्रमाणीकरण पद्धति विवरण में यथापरिभाषित प्रक्रिया, जिसके अंतर्गत पहचान और/या नियोजन, का सत्यापन भी है, की अनुपालना करेगा ;

(iii) सभी एकांतता अपेक्षाओं की अनुपालना करेगा ;

(iv) अंकीय चिह्नक प्रमाणपत्र का अनुरोध करने वाले व्यक्ति की सहमति प्राप्त करेगा कि ऐसे अंकीय चिह्नक प्रमाणपत्र के ब्यौरे किसी निदेशिका सेवा में प्रकाशित किए जा सकेंगे ।

26. प्रमाण पत्र की समयावधि—(1) कोई अंकीय चिह्नक प्रमाणपत्र,—

(क) अभिहित अवसान तारीख के साथ जारी किया जाएगा ;

(ख) जिसका निलम्बन किया गया है, प्रचालनात्मक उपयोग के लिए वापस किया जाएगा, यदि उसका निलम्बन अधिनियम की धारा 37 के अनुसार प्रत्याहृत किया जाता है ;

(ग) का अभिहित अवसान की तारीख को, जिसको अंकीय चिह्नक प्रमाणपत्र का पुराभंडारण किया जाता है, स्वतः अवसान हो जाएगा ;

(घ) का अवसान पर पुनःप्रयोग नहीं किया जाएगा ।

(2) उस अवधि का विस्तार नहीं किया जाएगा जिसके लिए कोई अंकीय चिह्नक प्रमाणपत्र जारी किया गया था किन्तु ऐसी अवधि के अवसान के पश्चात् नया अंकीय चिह्नक प्रमाणपत्र जारी किया जा सकेगा ।

27. अंकीय चिह्नक प्रमाणपत्र का पुरःअभिलेख- प्रमाणकर्ता प्राधिकारी,—

(क) अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए आवेदनों ;

(ख) उत्पादित अंकीय चिह्नक प्रमाणपत्रों के रजिस्ट्रीकरण और सत्यापन दस्तावेजों ;

(ग) अंकीय चिह्नक प्रमाणपत्रों ;

(घ) निलम्बन की सूचनाओं ;

(ङ) निलम्बित अंकीय चिह्नक प्रमाणपत्रों की सूचना ;

(च) प्रतिसंहृत अंकीय चिह्नक प्रमाणपत्रों की सूचना ;

(छ) अवसन्नित अंकीय चिह्नक प्रमाणपत्र,

का न्यूनतम सात वर्ष की अवधि के लिए या विधिक अपेक्षा के अनुसार अवधि के लिए अभिलेखन करेगा ।

28. अंकीय चिह्नक प्रमाणपत्रों का जोखिम में पड़ना-प्रचालनात्मक उपयोग में ऐसे अंकीय चिह्नक प्रमाणपत्रों का, जो जोखिम में पड़ गए हैं, प्रमाणकर्ता प्राधिकारी के प्रमाणीकरण पद्धति विवरण में परिभाषित प्रक्रिया के अनुसार प्रतिसंहरण किया जाएगा ।

स्पष्टीकरण : अंकीय चिह्नक प्रमाणपत्र—

(क) जोखिम में पड़ गए समझे जाएंगे जब—

(i) अंकीय चिह्नक प्रमाणपत्र से सहबद्ध प्राइवेट कुंजी की अखंडता शंका में है ;

(ii) अंकीय चिह्नक प्रमाणपत्र स्वामी की विश्वसनीयता शंका में है, जैसे कुंजी युग्मों का दोषपूर्ण या अवैध प्रयोजनों के लिए उपयोग या उपयोग करने का प्रयास या अन्यथा करना ;

(ख) केवल उस समय तक जोखिम में पड़ी स्थिति में रहेंगे जब तक उसके प्रतिसंहरण का इंतजाम नहीं हो जाता है ।

29. अंकीय चिह्नक प्रमाणपत्र का प्रतिसंहरण—(1) अंकीय चिह्नक प्रमाणपत्र का प्रतिसंहरण तब किया जाएगा और वे किसी निष्ठ उपयोग के लिए अवैध हो जाएंगे, जब—

(क) अंकीय चिह्नक प्रमाणपत्र स्वामी के प्राइवेट कुंजी के संबंध में कोई जोखिम है ;

(ख) अंकीय चिह्नक प्रमाणपत्र का दुरुपयोग हुआ है ;

(ग) अंकीय चिह्नक प्रमाणपत्र में कोई दुर्व्यपदेशन या गलती है ;

(घ) अंकीय चिह्नक प्रमाणपत्र अब और अपेक्षित नहीं है ।

(2) प्रतिसंहरण अंकीय चिह्नक प्रमाणपत्र, प्रमाणपत्र प्रतिसम्पहरण सूची (सी.आर.एल.) के साथ जोड़े जाएंगे ।

30. अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए फीस—(1) प्रमाणकर्ता प्राधिकारी, अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए ऐसी फीस प्रभारित कर सकेगा, जो केन्द्रीय सरकार द्वारा अधिनियम की धारा 35 की उपधारा (2) के अधीन विहित की जाए।

(2) प्रमाणपत्र के निकालने के लिए प्रमाणकर्ता प्राधिकारी के एक्स.500 के अभिगम की बाबत फीस संदेय हो सकेगी । जहां फीस संदेय है वहां प्रमाणकर्ता प्राधिकारी, अपने सभी हस्ताक्षरकर्ताओं और उपयोगकर्ताओं को अद्यतन फीस अनुसूची की व्यवस्था करेगा, जो किसी नामित वैबसाइट पर फीस अनुसूची के प्रकाशन द्वारा हो सकेगी ।

(3) प्रमाणपत्र प्रतिसंहरण या प्रास्थिति सूचना के लिए प्रमाणकर्ता प्राधिकारी के एक्स X.500 निर्देशिका सेवा के अभिगम की बाबत फीस संदेय हो सकेगी । जहां फीस संदेय हो वहां प्रमाणकर्ता प्राधिकारी अपने सभी हस्ताक्षरकर्ताओं और उपयोगकर्ताओं को अद्यतन फीस अनुसूची की व्यवस्था करेगा, जो किसी नामित वैबसाइट पर फीस अनुसूची के प्रकाशन द्वारा हो सकेगी ।

(4) इंटरनेट के माध्यम से प्रमाणीकरण पद्धति विवरण के अभिगम के लिए कोई फीस उद्ग्रहणीय नहीं होगी । किसी प्रमाणकर्ता प्राधिकारी द्वारा उसके प्रमाणीकरण पद्धति विवरण की मुद्रित प्रतियों की व्यवस्था करने के लिए फीस प्रभार्य हो सकती ।

31. संपरीक्षा—(1) प्रमाणकर्ता प्राधिकारी अपने प्रचालनों की वार्षिक संपरीक्षा किसी संपरीक्षक द्वारा कराएगा और ऐसी संपरीक्षा में अन्य बातों के साथ निम्नलिखित होंगे,—

(i) सुरक्षा नीति और योजना ;

(ii) भौतिक सुरक्षा ;

- (iii) प्रौद्योगिकी मूल्यांकन ;
- (iv) प्रमाणकर्ता प्राधिकारी की सेवाओं का प्रशासन ;
- (v) सुसंगत प्रमाणीकरण पद्धति विवरण ;
- (vi) सुसंगत प्रमाणीकरण पद्धति विवरण की अनुपालना ;
- (vii) संविदा/करार ;
- (viii) नियंत्रक द्वारा विहित विनियम ;
- (ix) प्रमाणकर्ता प्राधिकारी नियम, 2000 की नीतिगत अपेक्षाएं ।

(2) प्रमाणकर्ता प्राधिकारी,—

- (क) अपने प्रचालनों की सुरक्षा नीति, भौतिक सुरक्षा और योजना की अद्वार्धिक संपरीक्षा करेगा ।
- (ख) अपने निधानों की त्रैमासिक संपरीक्षा करेगा ।

(3) प्रमाणकर्ता प्राधिकारी, ऐसी संपरीक्षा के पूरा होने के चार सप्ताह के भीतर नियंत्रक को, प्रत्येक संपरीक्षा रिपोर्ट की प्रति प्रस्तुत करेगा और जहां कहीं अनियमितताएं पाई जाएं वहां प्रमाणकर्ता प्राधिकारी तुरंत ऐसी अनियमितताओं को दूर करने के लिए समुचित कार्रवाई करेगा ।

32. संपरीक्षक के प्रमाणकर्ता प्राधिकारी से संबंध—(1) संपरीक्षक संपरीक्षा किए जा रहे प्रमाणकर्ता प्राधिकारी से स्वतंत्र होगा और ऐसा साफ्टवेयर या हार्डवेयर विक्रेता नहीं होगा जिसने उक्त प्रमाणकर्ता प्राधिकारी की सेवा की है या कर रहा है या उसे उपस्करण का प्रदाय किया है या कर रहा है ।

(2) संपरीक्षक और प्रमाणकर्ता प्राधिकारी के ऐसे कोई चालू या नियोजित वित्तीय, विधिक या अन्य संबंध नहीं होंगे, जो संपरीक्षक या संपरीक्षा किए जा रहे पक्ष से भिन्न हो ।

33. गोपनीय सूचना—निम्नलिखित सूचना गोपनीय होगी, अर्थात् :—

- (क) अंकीय चिह्नक प्रमाणपत्र आवेदन चाहे अनुमोदित हो या अस्वीकृत ;
- (ख) रजिस्ट्रीकरण और सत्यापन अभिलेख के भाग रूप संगृहीत अंकीय चिह्नक प्रमाणपत्र सूचना, किन्तु जो अंकीय चिह्नक प्रमाणपत्र सूचना में सम्मिलित न हों ;
- (ग) हस्ताक्षरकर्ता करार ।

34. गोपनीय सूचना का अभिगम—(1) प्रमाणकर्ता प्राधिकारी के प्रचालन कर्मचारिवृन्द द्वारा गोपनीय सूचना का अभिगम “जानकारी की आवश्यकता” और “उपयोग की आवश्यकता” के आधार पर होगा ।

(2) नियम 33 में विहित सभी गोपनीय सूचना अंतर्विष्ट करने वाले कागज आधारित अभिलेख, प्रलेख और पूर्तिकर डाटा सुरक्षित और तालेबंद आधान या संविका प्रणाली में अन्य सभी अभिलेख से पृथक रखे जाएंगे ।

(3) गोपनीय सूचना उस मामले के सिवाय जहां समुचित सांविधानिक वारन्ट या अन्य वैध रूप से प्रवर्तनीय दस्तावेज नियंत्रक को प्रस्तुत किया जाता है और वह ऐसा अनुज्ञात करता है, देश से बाहर नहीं ले जाई जाएगी ।

अनुसूची-1

(नियम 10 देखिए)

प्रमाणकर्ता प्राधिकारी होने के लिए अनुज्ञाप्ति अनुदत्त करने के लिए आवेदन का प्ररूप
व्यष्टिक आवेदकों के लिए

1. पूरा नाम*

अंतिम नाम और उप नाम _____

प्रथम नाम _____

मध्य नाम _____

2. क्या आप सभी किसी अन्य नाम से जाने जाते रहे हैं ? यदि हां, तो
 अंतिम नाम/उपनाम

प्रथम नाम _____

मध्य नाम _____

3. पता

क. निवास स्थान का पता- *

फ्लैट/डोर/ब्लाक सं0 _____

परिसर/भवन/ग्राम का नाम _____

सड़क /स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थान/तालुका/उपखंड _____

नगर/शहर/जिला _____

राज्य/संघ राज्य क्षेत्र _____ पिन: _____

टेलीफोन सं0 _____

फैक्स _____

मोबाइल फोन नं0 _____

ख. कार्यालय पता *

कार्यालय का नाम _____

फ्लैट/डोर/ब्लाक सं0 _____

परिसर/भवन/ग्राम का नाम _____

सड़क/स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थान/तालुका/उपखंड _____

नगर/शहर/जिला _____ पिन: _____

राज्य/संघ राज्य क्षेत्र _____

फैक्स _____

4. पत्राचार के लिए पता :— *क ख जो लागू हो उस पर सही √ निशान लगाएं

5. पिता का नाम * _____

अंतिम नाम/उपनाम _____

प्रथम नाम _____

मध्य नाम _____

6. लिंग- * (व्यष्टि आवेदक के लिए) जो लागू हो उस पर सही √ निशान लगाएं : पुरुष/स्त्री

7. जन्म की तारीख(दिन/मास/वर्ष) * _____ / _____ / _____

8. राष्ट्रीयता * _____

9. क्रेडिट कार्ड के ब्यौरे _____

क्रेडिट कार्ड की किस्म _____

क्रेडिट कार्ड संख्याक _____

जारी करने वाले का नाम _____

10. ई मेल का पता _____

11. वेब यू आर एल पता _____

12. पासपोर्ट का ब्यौरा # _____

पासपोर्ट सं० _____

पासपोर्ट जारी करने वाला प्राधिकारी _____

पासपोर्ट के अवसान की तारीख (दिन/मास/वर्ष) _____ / _____ / _____

13. मतदाता का पहचान पत्र संख्यांक # _____

14. आयकर पेन संख्यांक # _____

15. आई एस पी का ब्यौरा* _____

आई एस पी का नाम * _____

आई एस पी के वेबसाइट का पता, यदि कोई हो _____

आई एस पी से आपका प्रयोग का नाम, यदि कोई हो _____

16. वैयक्तिक वेब पेज यू आर एल, पता यदि कोई हो _____

17. कारबार या वृत्ति में लगी पूँजी * _____

रु. _____

(दस्तावेजी सबूत संलग्न करें)

कंपनी/फर्म/व्यष्टिकों के निकाय/व्यक्तियों के संगम/स्थानीय प्राधिक नी/न्यास के निए

18. रजिस्ट्रीकरण संख्यांक * _____

19. निगमन/करार/भागीदारी की तारीख* _____ / _____ / _____

२० कारबार की विशिष्टियां, यदि कोई हैं _____

प्रधान कार्यालय _____

कार्यालय का नाम _____

फ्लैट/डोर/ब्लाक संख्या _____

परिसर/भवन /ग्राम का नाम _____

राडक/स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थासान/तालुका/उपप्रखंड _____

नगर/शहर/जिला _____

राज्य/संघ राज्य क्षेत्र _____ पिन: _____

टेलीफोन नं. _____

फैक्ट्र _____

वेब पेज यू आर एल पता, यदि कोई हो _____

शाखाओं की संख्या _____

कारबार की प्रकृति _____

21. आयकर पेन संख्यांक * _____

22. पिछले वित्तीय वर्ष का व्यापारावर्त रु. _____

23. शुद्ध स्वामित्व *
(दस्तावेजी सबूत संलग्न करें)

24. सदत पूंजी * रु. _____
(दस्तावेजी सबूत संलग्न करें)

25. बीमा के ब्यौरे _____
बीमा पॉलिसी सं. * _____

बीमाकर्ता कंपनी * _____

26. भागीदारों/सदस्यों/निदेशकों के नाम, पते आदि (अधिक व्यक्तियों की दशा में सूचना के लिए अगले पृष्ठ में किए गए निम्नलिखित प्ररूप में अतिरिक्त शीटें जोड़ें) *
भागीदारों/सदस्यों/निदेशकों की सं.
भागीदारों/सदस्यों/निदेशकों
के ब्यौरे _____

क. पूरा नाम _____
अंतिम नाम/उपनाम _____
प्रथम नाम _____
मध्य नाम _____

ख. पता
फ्लैट/डोर/ब्लाक सं. _____
परिसर/भवन/ग्राम का नाम _____

सड़क/स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थान/तालूका/उपप्रखंड _____

नगर/शहर/जिला _____

राज्य/संघराज्य क्षेत्र _____ पिन _____

टेलीफोन सं० _____

फैक्स सं० _____

मोबाइल फोन सं० _____

ग. राष्ट्रीयता

विदेशी राष्ट्रिक की दशा में, वीजा का व्यौरा _____

घ. पासपोर्ट का व्यौरा #

पासपोर्ट सं० _____

पासपोर्ट जारी करने वाला प्राधिकारी _____

पासपोर्ट के अवसान की तारीख _____

ड. मतदाता पहचान पत्र सं० # _____

च. आयकर पेन सं० # _____

छ. ई-मेल पता _____

ज. व्यक्तिक वेब पेज यू आर एल, यदि कोई हो _____

27. प्राधिकृत प्रतिनिधि *

नाम _____

फ्लैट/डोर/ब्लाक सं० _____

परिसर/भवन/ग्राम का नाम _____

सड़क/स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थान/तालूका/उपप्रखंड _____

नगर/शहर/जिला _____

राज्य/संघराज्य क्षेत्र _____ पिन _____

टेलीफोन सं० _____

फैक्स सं० _____

कारबार की प्रकृति _____

सरकारी मंत्रालय/विभाग/अभिकरण/प्राधिकारी के लिए

28. संगठन की विशिष्टियां *

संगठन का नाम _____

प्रशासकीय मंत्रालय/विभाग _____

राज्य/केन्द्रीय सरकार के अधीन _____

फ्लैट/डोर/ब्लाक सं० _____

परिसर/भवन/ग्राम का नाम _____

सड़क/स्ट्रीट/गली/डाकघर _____

क्षेत्र/अवस्थान/तालुका/उपप्रखंड _____

नगर/शहर/जिला _____

राज्य/संघराज्य क्षेत्र _____ पिन: _____

टेलीफोन सं0 _____

फैक्स सं0 _____

वेब पेज यू आर एल पता _____

संगठन के प्रधान का नाम _____

पदनाम _____

ई-मेल का पता _____

29. बैंक के ब्यारे

बैंक का नाम * _____

शाखा * _____

बैंक खाता संख्या * _____

बैंक खाते का प्रकार * _____

30. क्या अनुज्ञाप्ति के लिए बैंकड्राफ्ट/संदाय आदेश संलग्न किया गया है * : हां/नहीं यदि हां तो,

बैंक का नाम _____

ड्राफ्ट/संदाय आदेश सं0 _____

जारी करने की तारीख _____

रकम _____

31. अंकीय चिह्नक प्रमाणपत्र तैयार करने

के लिए भारत में सुविधा का अवस्थान * _____

32. लोक कुंजी @ _____

33. क्या बैंक प्रत्याभूति/निष्पादन बंधपत्र संलग्न किया गया है * : हां/नहीं

(यदि आवेदक सरकारी मंत्रालय/विभाग/अभिकरण/प्राधिकारी है तो यह लागू नहीं होगा)

34. क्या प्रमाणन व्यवहार विवरण संलग्न किया गया है * : हां/नहीं

35. क्या कारबार रजिस्ट्रीकरण दस्तावेज की प्रमाणित प्रतियां संलग्न की गई हैं : हां/नहीं

(कंपनी/फर्म/व्यष्टिक निकाय/व्यक्ति संगम/स्थानीय प्राधिकारी के लिए)

यदि हां, तो दस्तावेज संलग्न करें :

(i) _____

(ii) _____

(iii) _____

36. कोई अन्य सूचना

तारीख

आवेदक के हस्ताक्षर

अनुदेशः 1. * से चिह्नांकित कॉलम आङ्गापक है ।

2. # से चिह्नांकित कॉलमों में कम-से-कम एक कॉलम में विवरण देना अनिवार्य है ।
3. कॉलम संख्या 1 से 17 तक व्यष्टिक आवेदकों द्वारा भरे जाने हैं ।
4. कॉलम संख्या 18 से 27 तक हिन्दू अधिभक्त कुटुंब आवेदकों द्वारा भरे जाने हैं यदि वे कपनी/फर्म/व्यष्टिकों का निकाय/व्यक्तियों का संगम/स्थानीय प्राधिकारी हैं ।
5. कॉलम 28 भरा जाना है यदि आवेदक सरकारी संगठन है ।
6. कॉलम संख्या 29, 30, 31 और 34 सभी आवेदकों द्वारा भरे जाने हैं ।
7. @ कालम सं0 32 केवल अनुज्ञाप्ति के नवीकरण के आवेदन के लिए लागू होता है ।
8. कालम सं0 33, यदि आवेदक सरकारी संगठन है तो लागू नहीं होता है ।

अनुसूची - 2

(नियम 19(2) देखिए)

सूचना प्रौद्योगिकी (सू.प्रौ.) सुरक्षा के मार्गदर्शक सिद्धांत

अनुक्रमणिका

	पृष्ठ
1. प्रस्तावना	22
2. सूचना सुरक्षा कार्यक्रम का कार्यान्वयन	22
3. सूचना वर्गीकरण	23
4. प्राकृतिक और परिचालन सुरक्षा	24
4.1 स्थल डिजाइन	24
4.2 अग्नि संरक्षण	24
4.3 पर्यावरणीय संरक्षण	24
4.4 वस्तुगत अभिगम	25
5. सूचना प्रबंधन	25
5.1 प्रणाली प्रशासन	25
5.2 संवेदनशील सूचना नियन्त्रण	26
5.3 संवेदनशील सूचना सुरक्षा	27
5.4 अन्य पक्षकार का अभिगम	27
5.5 कम्प्यूटर के दुरुपयोग का निवारण	27

6.	प्रणाली की अक्षतता और सुरक्षा उपाय	28
6.1	सुरक्षा प्रणालियों या सुविधाओं का उपयोग	28
6.2	प्रणाली अभिगम नियंत्रण	28
6.3	संकेत शब्द प्रबंधन	29
6.4	विशेषाधिकार प्राप्त उपयोगकर्ता का प्रबंध	30
6.5	उपयोगकर्ता का लेखा प्रबंधन	30
6.6	डाटा और साधन संरक्षण	31
7.	संवेदनशील प्रणालियों का संरक्षण	31
8.	डाटा केन्द्र के प्रचालन की सुरक्षा	31
8.1	कार्य नियतन	31
8.2	प्रणाली के प्रचालन की प्रक्रिया	32
8.3	मीडिया प्रबंधन	32
8.4	मीडिया संचलन	32
9.	डाटा बैकअप और अवस्थलीय प्रतिधारण	33
10.	संपरीक्षा ट्रेल्स और सत्यापन	33
11.	कंप्यूटर वायरस से निपटने के लिए उपाय	34
12.	हार्डवेयर और सॉफ्टवेयर का पुनर्स्थापन	35
13.	हार्डवेयर और सॉफ्टवेयर का रखरखाव	35
14.	हार्डवेयर और सॉफ्टवेयर का क्रय और अनुज्ञापन	36
15.	प्रणाली सॉफ्टवेयर	36
16.	प्रलेखन सुरक्षा	37
17.	नेटवर्क संसूचना सुरक्षा	37
18.	फायरवाल्स	38
19.	संयोजकता	38
20.	नेटवर्क प्रशासक	38
21.	परिवर्तन प्रबंधन	39
21.1	परिवर्तन नियंत्रण	39
21.2	उत्पादन प्रणाली के लिए परिवर्तनों का परीक्षण	39
21.3	परिवर्तन का पुनर्विलोकन	39
22.	समस्या प्रबंधन और रिपोर्टिंग	40
23.	आपातकालीन तैयारी	40
24.	आकस्मिकता प्रत्युद्धरण उपस्कर और सेवाएं	40
25.	सुरक्षा घटना का रिपोर्ट किया जाना तथा प्रतिक्रिया ।	40
26.	आपदा प्रत्युद्धरण/प्रबंध	41

अनुसूची-2सूचना प्रौद्योगिकी (सू.प्रौ.) सुरक्षा के मार्गदर्शक सिद्धान्त1. प्रस्तावना

इस दस्तावेज में सूचना प्रौद्योगिकी सुरक्षा के कार्यान्वयन और प्रबंधन के लिए प्रक्रिया और मार्गदर्शक सिद्धान्त उपबन्धित हैं। सुरक्षा अपेक्षाओं की अन्तर्निहित गतिकता के कारण इस दस्तावेज में एकदम सही सांचा उपबंधित नहीं किया जा सकता जिसका संगठनों द्वारा पालन किया जाना है। तथापि, मार्गदर्शनों के लिए सुरक्षा प्रणाली का उपयुक्त और पर्याप्त सांचा उपबंधित किया जा रहा है। संगठनों का यह दायित्व है कि वे आन्तरिक ऐसी प्रणाली विकसित कर जो इस दस्तावेज में वर्णित प्रक्रिया और मार्गदर्शक सिद्धान्तों के अनुकूल हों।

सूचना प्रौद्योगिकी सुरक्षा प्रक्रिया और मार्गदर्शन में प्रयुक्त निम्नलिखित शब्दावली का निम्नलिखित रूप में अर्थान्वयन किया जाएगा।

गा, गी, गे परिभाषित मार्गदर्शन आज्ञापक अपेक्षा है और इसलिए उसका पालन किया जाएगा।

चाहिए जहा समुचित, प्रतिकारी नियंत्रण कार्यान्वयित किए जाएंगे वहां परिभाषित मार्गदर्शन एक सिफारिश की गई अपेक्षा है। इसका अननुपालन प्रलेखीकृत किया जाएगा और प्रबन्धन द्वारा अनुमोदित किया जाएगा।

होगा परिभाषित प्रक्रिया और मार्गदर्शन आमापक अपेक्षा है और इसलिए इनका पालन किया जाएगा।

सकेगा परिभाषित मार्गदर्शन वैकल्पिक अपेक्षा है। इस मार्गदर्शन सिद्धान्त का कार्यान्वयन संगठन की अपेक्षा के अनुसार अवधारित किया जाता है।

2. सूचना सुरक्षा कार्यक्रम का कार्यान्वयन

अर्थपूर्ण सूचना सुरक्षा कार्यक्रम का सफल कार्यान्वयन उच्च स्तर के प्रबंधक के सहयोग पर निर्भर करता है। जब तक संगठन के वरिष्ठ प्रबंधक सूचना सुरक्षा कार्यक्रमों के उद्देश्यों को नहीं समझते और उनसे सहमत नहीं होते तब तक इसकी अतिम सफलता प्राप्त नहीं की जाएगी।

सूचना सुरक्षा कार्यक्रम को निम्नलिखित विनिर्दिष्ट प्रक्रमों में विभाजित कियों जाना चाहिए;

- (क) सुरक्षा नीति को अपनाना
- (ख) सुरक्षा जोखिम का विश्लेषण
- (ग) सूचना वर्गीकरण प्रणाली का विकास और कार्यान्वयन
- (घ) सुरक्षा मानक मैनुअल का विकास और कार्यान्वयन
- (ङ) प्रबंधन सुरक्षा की स्व-निर्धारण की प्रक्रिया का कार्यान्वयन
- (च) चालू सुरक्षा कार्यक्रम का अनुस्करण और प्रवर्तन
- (छ) प्रशिक्षण

सुरक्षा कार्यान्वयन का मुख्य कार्य संगठन के भीतर व्यक्तियों की जिम्मेदारी को सुनिश्चित करना है। कार्यान्वयन इस सामान्य सिद्धान्त पर आधारित होना चाहिए कि वह व्यक्ति जो सूचना उत्पादित कर रहा है, उसकी सुरक्षा के लिए भी जिम्मेदार है। तथापि, उसे इस संबंध में अपनी जिम्मेदारियों को निभाने में समर्थ बनाने के लिए आवश्यक उचित उपकरण और पर्यावरण स्थापित करने होंगे।

जब किसी एक स्तर पर सूचना के विभिन्न दुकङ्गों को उच्चतर कीमत की सूचना के रूप में एकीकृत किया जाता है तब इसकी सुरक्षा की आवश्यकताओं के बारे में जिम्मेदारी पदानुक्रम में समाकलक तक जानी चाहिए और इसके अभिगम के लिए उच्च स्तर का अधिकारी अपेक्षित है। प्रत्येक सूचना की बाबत यह अनन्य रूप से स्पष्ट होना

इसके अभिगम के लिए उच्च स्तर का अधिकारी अपेक्षित है। प्रत्येक सूचना की बाबत यह अनन्य रूप से स्पष्ट होना चाहिए कि उसका स्वामी, उसका संरक्षक और उसका उपयोगकर्ता कौन है। उसके स्वामी का यह कर्तव्य है कि वह सूचना का सही वर्गीकरण समनुदेशित करे जिससे सुरक्षा का अपेक्षित स्तर प्रवर्तित किया जा सके। सूचना का अभिरक्षक सुरक्षा मार्गदर्शनों के उचित कार्यान्वयन और इस बात जो लिए जिम्मेदार है कि वह उपयोगकर्ताओं को, जानने की आवश्यकता के आधार पर सूचना उपलब्ध कराए।

3. सूचना वर्गीकरण

सूचना आस्तियों को उनकी संवेदनशीलता और संगठन के लिए उनके महत्व के आधार पर वर्गीकृत किया जाएगा। चूंकि प्रबंधकों और कर्मचारियों से यह अपेक्षा करना काल्पनिक है कि वे संगठन की चारदीवारी के भीतर सभी सूचना के ऊपर पूर्ण नियंत्रण रखें, इसलिए उनको यह सलाह देना आवश्यक है कि किस किस्म की सूचना को अधिक संवेदनशील समझे और संवेदनशील सूचना का संगठन किस प्रकार रखरखाव और सुरक्षा करना चाहता है। वर्गीकृत डाटा के वर्गीकरण, पुनः एकीकरण, लेबल लगाने, भंडार करने, अभिगम, विनाश और पुनः उत्पादन पर जिसके लिए प्रशासनिक शिरोपरि प्रक्रिया सृजित की जाएगी पर कैसे ध्यान रखें। वर्गीकृत सूचना के मूल्य और उस प्रशासनिक भार के बीच जो वर्गीकरण प्रणाली संगठन पर डालती है, संलुतन बनाए रखने में असफलता के परिमाणस्वरूप इसमें सफलता प्राप्त करने में दीर्घकालीन कठिनाइयां उत्पन्न होंगी।

गोपनीयता सूचना का वह वर्गीकरण है जिसके अप्राधिकृत प्रकटन / उपयोग से संगठन के लिए गंभीर हानि हो सकती है, उदाहरणार्थ युद्धनीति योजना से संबंधित दस्तावेज।

निर्बंधित सूचना का वह वर्गीकरण है जिसका अप्राधिकृत प्रकटन / उपयोग संगठन और / या इसके ग्राहकों से सर्वोत्तम हित में नहीं होगा, उदाहरण के लिए डिजाइन, विकरण, कंप्यूटर साफ्टवेयर (कार्यक्रम उपयोगिताएं) प्रलेखीकरण, संगठन के कार्मिकों का डाटा, बजट सूचना।

आंतरिक प्रयोग सूचना का वह वर्गीकरण है जो कंपनी के भीतर प्रकटन के विरुद्ध किसी डिग्री का संरक्षण अपेक्षित नहीं है, उदाहरण के लिए प्रचालन प्रक्रियाएं, नीतियां और मानक अंतकार्यालय ज्ञापन।

अवर्गीकृत सूचना का वह वर्गीकरण है जो प्रकटन के विरुद्ध किसी संरक्षण की अपेक्षा नहीं करता है, उदाहरण के लिए प्रकाशित वार्षिक रिपोर्ट और पत्रिकाएं।

जब किसी साधारण संगठन के दृष्टिकोण से उपरोक्त वर्गीकरण उचित हों तब निम्नलिखित वर्गीकरणों पर विचार किया जा सकेगा :

परम गुप्त : यह उस सूचना को लागू होगा जिसके अप्राधिकृत प्रकटन से राष्ट्रीय सुरक्षा या राष्ट्रीय हित को असाधारण रूप से गंभीर क्षति होने की प्रत्याक्षा की जा सकती है। यह प्रवर्ग राष्ट्र के अत्याधिक गुप्त मुद्दों के लिए आरक्षित है और इसका बड़ी सावधानी से उपयोग किया जाना चाहिए।

गुप्त : यह उस सूचना को लागू होगा जिसके अप्राधिकृत प्रकटन से राष्ट्रीय सुरक्षा और राष्ट्रीय हित को गंभीर क्षति कारित होने या इसके कार्यकर्त्ता में गंभीर हस्तक्षेप कारित होने की प्रत्याशा है। इस वर्गीकरण का अत्याधिक महत्व की सूचना के लिए उपयोग किया जाना चाहिए और यह सामान्यतः उच्चतम वर्गीकरण है।

गोपनीयता : यह उस सूचना को लागू होगी जिसके अप्राधिकृत प्रकटन से संगठन की सुरक्षा को क्षति होने की प्रत्याक्षा है या जिससे संगठन के हितों पर प्रतिकूल प्रभाव पड़ने की संभावना हो या यह संगठन के कार्यकरण को प्रभावित करता हो। अधिकांश सूचना को, उचित विश्लेषण के पश्चात्, गोपनीयता से अधिक ऊंचे स्तर में वर्गीकृत नहीं किया जाए।

निर्बंधित : यह ऐसी सूचना को लागू किया जाएगा जो केवल शासकीय उपयोग के लिए ही है और जो शासकीय प्रयोजनों के अलावा किसी प्रयोजन के लिए प्रकाशित या संसूचित नहीं की जाएगी।

अवर्गीकृत : यह सूचना का ऐसा वर्गीकरण है जो प्रकटन के विरुद्ध किसी संरक्षण की अपेक्षा नहीं करता।

4. प्राकृतिक और परिचालन सुरक्षा

4.1. स्थल डिजायन

(1) स्थल ऐसे स्थानों में नहीं होगा जो बाढ़, अग्नि, रासायनिक संदूषण और विसफोटों की तरह के प्राकृतिक और कृत्रिम संकटों के प्रति प्रणत हों ।

(2) प्रचालनों की प्रकृति के अनुसार, उपयुक्त तल संरचना, प्रकाश, विद्युत और जल हानि संरक्षण अपेक्षाओं की व्यवस्था की जाएगी ।

(3) सन्निर्माण लागू होने वाले उन सभी भवन और सुरक्षा विनियमों के अनुरूप होगा जो सुसंगत सरकारी अभिकरणों द्वारा अधिकथित और निर्माण टैम्पर-एविडेट होना चाहिए ।

(4) प्रचालन स्थल के सन्निर्माण केलिए उपयोग की गई सामग्री अग्निरोधी और विषेश रसायनों से मुक्त होगी ।

(5) बाहरी दीवारें इंटों से निर्मित होंगी या किसी प्रबल हमले का प्रतिरोध करने की क्षमता वाले पर्याप्त रूप से मोटी कंक्रीट की होंगी । भूतल पर खिड़कियां मजबूत मृत स्टील की गिल से ढकी होंगी या संघात सोधी परतवार सुरक्षा कांच की होंगी । सभी आंतरिक दीवारें फर्श से छत तक होंगी और टैम्पर-एविडेट होंगी ।

(6) वातानुकूलन प्रणीती, विद्युत प्रदाय प्रणाली और उचित बैकअप के साथ निर्विधन विद्युत प्रदाय यूनिट प्रचालन की प्रकृति पर आधारित रूप में स्थापित की जाएगी । वातानुकूलन प्रणाली के सभी डाकिंग होल्स् ऐसी डिजाइन के होने चाहिए जिससे किसी प्रकार की गुटर्फेंट को रोका जा सके ।

(7) स्वचालित अग्नि संसूचन और अग्नि दमन प्रणाली तथा ऐसे उपस्कर जो अग्निशमन दल द्वारा या केन्द्र या राज्य सरकार के किसी अन्य अभिकरण द्वारा विनिर्दिष्ट अपेक्षा के अनुरूप हैं, प्रचालन स्थल पर स्थापित किए जाएंगे ।

(8) मीडिया पुस्तकालय, विद्युत और यांत्रिक नियंत्रण कक्ष पृथक एकांत क्षेत्र में स्थापित किए जाएंगे जिन तक पहुंचने की अनुमति विनिर्दिष्ट, नामित व्यष्टियों को आवश्यकता के अनुसार प्रदान की जाएगी ।

(9) ऐसी सुविधा जो मिशन-नाजुक और संवेदनशील उपयोजनों की सहायता करती है, ऐसे स्थान पर और ऐसी डिजाइन में होगी जो मरम्मत किए जाने, दुसरे स्थान पर स्थापित किए जाने और पुनःसंस्थित किए जाने योग्य हो । इन उपयोजनों को पुनःअवस्थित, पुनःसंगठित और पुनःसंस्थित करने की क्षमता की कारबार निरन्तरता/ संकट बचाव योजना के भाग के रूप में समीक्षा की जाएगी ।

4.2. अग्नि संरक्षण

(1) प्रचालन स्थल के सौ (100) मीटर के भीतर ज्वलनशील सामग्री भंडारित नहीं की जाएगी ।

(2) अग्निशमन दल या केन्द्रीय या राज्य सरकार के किसी अन्य अभिकरण द्वारा यथा विहित स्वाचालित अग्नि संसूचन और अग्नि दमन प्रणालियां और श्रव्य संकटघटियां प्रचालन स्थल पर लगायी जाएंगी ।

(3) अग्निशमक प्रचालन स्थल पर लगा जाएंगे और उनकी अवस्थिति समुचित चिह्नों द्वारा स्पष्ट रूप से अंकित की जाएंगी ।

(4) अग्नि उपस्कर और अग्नि दमन प्रणालियों का सावधिक परीक्षण, निरीक्षण और अनुरक्षण किया जाएगा ।

(5) आपात स्थिति में कार्मिकों के सुरक्षित निष्क्रमण के लिए प्रक्रिया प्रचालन स्थल पर मुख्य स्थानों पर दृश्यमान रूप में चिपकाई /प्रदर्शित की जाएंगी । सावधिक प्रशिक्षण और अग्नि ड्रिल की जाएंगी ।

(6) परिचालन स्थल में कोई भी खाना पीना या धूम्रपान नहीं किया जाएगा । कार्यस्थल हर समय साफ रखा जाएगा ।

4.3. पर्यावरणीय संरक्षण

(1) संपूर्ण परिचालन स्थल में ऊपर उठाए गए तल के नीचे जल संसूचक स्थापित किया जाएगा और उसे शृंख्य घंटियों से जोड़ा जाएगा ।

(2) परिचालन स्थल में तापमान और आद्रता की दशा का मानिटर और नियंत्रण सावधिक रूप से किया जाएगा ।

(3) परिचालन स्थल पर कार्मिकों को अग्नि और पर्यावरण संरक्षण के प्रयोजन हेतु परिचालन स्थल पर स्थापित विभिन्न उपस्कर और युक्तियों का मानिटर और नियंत्रण करने का प्रशिक्षण दिया जाएगा ।

(4) उपस्कर और प्रणालियों के सावधिक निरीक्षण, परीक्षण और अनुरक्षण नियत किया जाएगा ।

4.4. वस्तुगत अभिगम

(1) प्रचालन के लिए प्रयुक्त प्रणालियों की वस्तुगत सुरक्षा और प्रचालन स्थल पर वस्तुगत अभिन्यास के लिए हर समय वर्ष में तीन सौ पैसठ दिन और सप्ताह में सातों दिन की जिम्मेदारी निश्चित की जाएगी और नामित व्यक्तियों को समनुदेशित की जाएगी ।

(2) प्रचालन स्थल पर अभिगम को नियंत्रित करने और उसकी संपरीक्षा करने के लिए जीव सांख्यिकी वस्तुगत अभिगम सुरक्षा प्रणाली स्थापित की जाएगी ।

(3) प्रचालन स्थल पर वस्तुगम अभिगम, हर समय, केवल प्राधिकृत कार्मिकों तक ही नियंत्रित और निर्बद्धित किया जाएगा । सीमित वस्तुगम अभिगम के लिए प्राधिकृत कार्मिकों को प्रचालन स्थल के अन्दर निर्बद्धित क्षेत्र में अप्राधिकृत अभिगम अभिप्राप्त करने के लिए अनुज्ञात नहीं किया जाएगा ।

(4) डाटा केन्द्र में सामान्य कारबार के घंटों के दौरान सूची और अभिगम कार्ड / कुंजी जारी करने के ऊपर दुहरा नियंत्रण सहीं तरह से होगा । ऐसे कार्मिकों की जिनके पास कार्ड / कुंजीयां हैं, अद्यतन सूची 3 वर्ष की अवधि के लिए नियमित रूप से रखी जाएगी और अभिलेखीकृत की जाएगी ।

(5) कार्ड / कुंजीयों के खो जाने की प्रचालन स्थल के सुरक्षा प्रयोक्षक को तत्काल रिपोर्ट की जाएगी जो अप्राधिकृत अभिगम को रोकने के लिए समुचित कार्रवाई करेगा ।

(6) प्रचालन कर्मचारिवृन्द से भिन्न सभी व्यक्ति प्रचालन स्थल में प्रवेश करते समय और उससे बाहर आते समय अपने हस्ताक्षर करेंगे और उनके साथ प्रचालन कर्मचारिवृन्द रहेंगे ।

(7) आपात निकास की सावधिक रूप से यह सुनिश्चित करने के लिए परीक्षा की जाएगी कि अभिगम प्रणाली प्रवर्तन में है ।

(8) डाटा केंद्रों के सभी प्रवेशों पर हर समय निगरानी वीडियो केमरों द्वारा मानीटर की जाएगी ।

5. सूचना प्रबन्धन

5.1. प्रणाली प्रशासन

(1) प्रत्येक संगठन समुचित रूप से प्रशिक्षित “प्रणाली प्रशासक” अभिहित करेगा जो यह सुनिश्चित करेगा कि प्रणाली के सुरक्षा संरक्षण उपाय सही कार्य कर रहे हैं और जो अपनी सुरक्षा मुद्रा बनाए रखेगा । किसी प्रणाली या उपयोजन की विविधता और सुरक्षा की आवश्यकताओं पर निर्भर रहते हुए प्रणाली प्रशासक के पास एक अभिहित प्रणाली सुरक्षा प्रशासक होगा जो सुरक्षा के दायित्वों को संभालेगा और सूचना को वस्तुगत, तार्किक प्रक्रिया संबंधी रखोपाय उपलब्ध कराएगा ।

(2) संगठन यह सुनिश्चित करेंगे कि केवल उचित रूप से प्रशिक्षित प्रणाली सुरक्षा प्रशासक को ही प्रणाली सुरक्षा के दायित्व सौंपे गए हैं ।

(3) सूचना का सृजन, वर्गीकरण, पुनः प्राप्त करने, उपन्तरण, लोप या लेखबद्ध करने की जिम्मेदारी प्रणाली प्रशासक पर ही होगी ।

(4) प्रणाली प्रशासन के लिए प्रयुक्त किसी संकेत शब्द को और न्यासित सेवाओं का प्रचालन लिखा जाना नहीं चाहिए (कागज या इलेक्ट्रॉनिक रूप में) या किसी को बताना नहीं चाहिए । संकेत शब्द प्रबंधन के लिए प्रणाली ऐसे स्थान पर होनी चाहिए जिससे सभी संभाव्यताओं को कवर करती हो जैसे भूले हुए संकेत शब्द या प्रणाली प्रशासक की दशा में किसी व्यक्ति को बदलना (या प्रणाली सुरक्षा प्रशासक) प्रशासक के संकेत शब्दों के उपयोग की प्रत्येक घटना को प्रलेखीकृत किया जाए ।

(5) सभी उपयोगकर्ताओं के अभिगम अधिकारों की सावधिक समीक्षा की जाना चाहिए ।

(6) प्रणाली प्रशासक, यदि उपयोगकर्ता की इस रूप में पहचान की जाती है कि उसने डाटा केन्द्र छोड़ दिया है, कार्यभार को बदल लिया है या उसे प्रणाली अभिगम की अब उसे आवश्यकता नहीं है तो उपयोगकर्ता के खाते तक पहुंच को तत्काल बन्द कर देगा । उपयोगकर्ता के खाते का पुनः सक्रियकरण प्रणाली प्रशासक द्वारा लिखित में प्राधिकृत किया जाएगा (अंकीय रूप से चिन्हित ई-मेल स्वीकार्य होगा) ।

(7) प्रणाली प्रशासक, उसके स्वामी द्वारा यथा विहित वर्गीकृत सूचना के रक्षापायों के कदम उठाएगा ।

(8) प्रणाली प्रशासक उपयोगकर्ताओं की विशेषाधिकार प्राप्त पहुंच को केवल जानकारी प्राप्त करने और ऐसे करने की आवश्यकता के आधार पर ही प्राधिकृत करेगा और उस प्राधिकरण के विलेखीकृत किए जाने के पश्चात् ही प्राधिकृत करेगा ।

(9) संपरीक्षा ट्रेलर्स/अभिगम लॉग की समीक्षा, अभिगम के अतिक्रमण की रिपोर्ट करने के मानदंड और समयबद्ध प्रबन्धन कार्य/जवाब को सुनिश्चित करने के लिए प्रक्रियाएं स्थापित की जाएंगी और विलेखीकृत की जाएंगी ।

(10) सभी सुरक्षा अतिक्रमणों को लेखबद्ध किया जाएगा और उनका अन्वेषण किया जाएगा तथा प्रबन्ध द्वारा समीक्षा के लिए प्रास्तित रिपोर्ट तैयार की जाएगी ।

(11) प्रणाली प्रशासक प्रणाली सहायक कर्मचारिवृन्द के साथ सूचना के संरक्षण में किसी कमजोरी के बारे में रिपोर्ट और पहचान की गई समस्याओं का नियमित विश्लेषण करेगा ।

(12) प्रणाली प्रशासक यह सुनिश्चित करेगा कि डाटा, फाइल और लोक कुंजी अवसंरचना (पी के आई) सरवर मानीटर किए बिना तो नहीं छोड़ दिए गए जब इन प्रणालियों को चालू कर दिया गया हो ।

(13) प्रणाली प्रशासक यह सुनिश्चित करेगा कि प्रणाली पर कोई निर्विशेष उपयोगकर्ता समर्थ या सक्रिय नहीं किया गया है ।

5.2. संवेदनशील सूचना नियंत्रण

(1) सूचना आस्तियों को उनकी संवेदनशीलता और संगठन के लिए उनकी नाजुकता के अनुसार वर्गीकृत और संरक्षित किया जाएगा ।

(2) इन मार्गदर्शक सिद्धान्तों के पैरा 8.3 के अनुसार प्रक्रियाएं भंडार मीडिया के रखरखाव के लिए सही होनी चाहिए जिनमें संवेदनशील और वर्गीकृत सूचना रखी गई हो ।

(3) किसी मीडिया में भंडारित संवेदनशील सभी सूचना पर कोई समुचित सुरक्षा वर्गीकरण डाला जाएगा या उसे समनुदेशित किया जाएगा ।

(4) सभी संवेदनशील सामग्री पर तदनुसार मुद्रा या लेबल लगाया जाएगा ।

(5) भंडारित मीडिया (अर्थात् फ्लापी डिस्केट्स, चुम्बकीय टेप, वहनीय हार्डडिस्क, आप्टीकल डिस्क आदि) जिनमें संवेदनशील सूचना अन्तर्विष्ट है, उनके वर्गीकरण के अनुसार संरक्षित किया जाएगा ।

(6) इलैक्ट्रॉनिक संसूचना प्रणाली जैसे रूटर, स्विचें, नेटवर्क, युक्ति और कंप्यूटर, जिनका उपयोग संवेदनशील सूचना के पारेषण के लिए किया जाता है, उपयुक्त सुरक्षा साफ्टवेयर से लैस या के साथ और यदि आवश्यक हो तो गूढ़ लेखन या गूढ़ लेखन साफ्टवेयर के साथ स्थापित की जाएंगी । इस संबंध में उपयुक्त प्रक्रिया प्रलेखीकृत की जाएगी ।

(7) प्रक्रियाएं आन्तरिक (हार्ड डिस्क/आटीकल डिस्क) या बाहरी (डिस्केट, डिस्क ड्राइव, टेप आदि) दोनों ही तरह से सभी विकृत/क्षतियुक्त या प्रभावित मीडिया पर संवेदनशील सूचना आस्तियों के व्ययन को सुनिश्चित करने के लिए प्रणाली में यथावत् होंगी। अधिमानतः प्रणाली में आन्तरिक या बाहरी रूप से ऐसे प्रभावित/विकृत या क्षतिग्रस्त मीडिया को नष्ट कर दिया जाएगा।

5.3 संवेदनशील सूचना सुरक्षा

(1) अत्यधिक संवेदनशील सूचना आस्तियां सुरक्षित स्थानान्तरणीय मीडिया में भंडारित की जाएंगी और अप्राधिकृत व्यक्तियों के हस्तक्षेप से बचने के लिए गूढ़ लेखन रूप में होनी चाहिए।

(2) अत्यधिक संवेदनशील सूचना पैरा 3 के अनुसार वर्गीकृत की जाएगी।

(3) संवेदनशील सूचना और डाटा की जो एक निश्चित कंप्यूटर डिस्क में भंडारित हैं जिसमें एक से अधिक व्यक्तियों का हिस्सा है, अभिगम नियंत्रण साफ्टवेयर (संकेत शब्द) द्वारा संरक्षा की जाएगी। सुरक्षा पैकेज ऐसे स्थापित किए जाएंगे जो पृथक् निर्देशिका/फाइलों के बारे में प्राधिकार प्रदान करेंगे और उनकों पृथक्-पृथक् करेंगे।

(4) हस्तान्तरणीय इलैक्ट्रॉनिक भंडार मीडिया कंप्यूटर से हटा लेना चाहिए और कार्य के सत्र या कार्य दिवस के अन्त में उचित रूप से सुरक्षित रखा जाना चाहिए।

(5) ऐसे स्थानान्तरणीय इलैक्ट्रॉनिक भंडार मीडिया पर जिसमें संवेदनशील सूचना और डाटा अन्तर्विष्ट हैं, स्पष्ट रूप से लेबल लगाया जाना चाहिए और उसकी सुरक्षा की जानी चाहिए।

(6) ऐसे हार्ड डिस्कों को जिनमें संवेदनशील सूचना और डाटा अन्तर्विष्ट हैं, कंप्यूटर प्रणाली को किसी अन्य आन्तरिक या बाहरी विभाग को रखरखाव के लिए देने से पूर्व साफ कर देना चाहिए।

5.4. अन्य पक्षकार का अभिगम

(1) कंप्यूटर प्रणाली में अन्य संगठनों द्वारा अभिगम सुरक्षा संरक्षण और नियंत्रणों के ऐसे ही स्तर के अध्यधीन होगा जैसा कि इन सूचना प्रोटोकोलीकी सुरक्षा मार्गदर्शक सिद्धान्तों में है।

(2) उस दशा में जहां डाटा केन्द्र अपने किसी प्रचालन के लिए बाहरी सेवा/सुविधा प्रदाता (बाह्य स्रोत) की सुविधाओं का उपयोग करता है, वहां बाहरी सेवा/सुविधा प्रदाता (बाह्य स्रोत) के उपयोग का संभावित सुरक्षा अरक्षितता और उसमें अन्तर्विलित जोखिमों को ध्यान में रखते हुए मूल्यांकन किया जाएगा। तथा ऐसे सभी करारों का सूचना आस्ति स्वामी द्वारा अनुमोदन किया जाएगा। बाहरी सेवा या सुविधा प्रदाता डाटा केन्द्र/प्रचालन स्थल के प्रबंधक के साथ अप्रकटन के करारों पर हस्ताक्षर करेगा।

(3) बाहरी सेवा / सुविधा प्रदाता (बाह्य स्रोत) उस सुरक्षा नियंत्रण के समान स्तर की व्यवस्था करेगा जो इन सूचना प्रोटोकोलीकी सुरक्षा मार्गदर्शक सिद्धान्तों द्वारा अपेक्षित हैं।

5.5. कंप्यूटर के दुरुपयोग का निवारण

(1) कंप्यूटरों और कंप्यूटर सूचना की उसके दुरुपयोग से सुरक्षा करने के लिए निवारण, पता लगाने और भयोपरकारी उपाय लागू किए जाएंगे। इस प्रकार किए गए उपायों को उचित रूप से प्रलेखीकृत किया जाएगा और उनकी नियमित रूप से समीक्षा की जाएगी।

(2) प्रत्येक संगठन सभी व्यक्तियों को जिनके अन्तर्गत प्रबंध, प्रणाली संवर्धक और कार्यक्रमक अन्तिम उपयोगकर्ता और अन्य उपयोगकर्ता भी हैं, कंप्यूटरों के दुरुपयोग के विरुद्ध चेतावनी देते हुए पर्याप्त सूचना उपलब्ध कराएगा।

(3) प्रत्येक संगठन के भीतर सुरक्षा भंगों के साथ शीघ्रता से निपटने के लिए प्रभावी उपाय स्थापित किए जाएंगे। ऐसे उपायों के अन्तर्गत निम्नलिखित होंगे :—

(i) आशंकित भंग की शीघ्रता से रिपोर्ट करना ;

- (ii) प्रत्याशित भंग की प्रकृति का उचित अन्वेषण और निर्धारण ;
- (iii) साक्ष्य प्राप्त करना और ऐसी सामग्री की जो किसी भंग की खोज से संबंधित है, अक्षतता कायम रखना ;
- (iv) उपचारिक उपाय ।

(4) भंगों से संबंधित सभी घटनाओं की, भविष्य में होने वाली घटनाओं की पुनरावृति को रोकने के लिए उपयुक्त कार्रवाई करने हेतु प्रणाली प्रशासक या प्रणाली सुरक्षा प्रशासक को रिपोर्ट की जाएगी ।

(5) प्रत्येक अभिकथित दुरुपयोग की प्रकृति को सिद्ध करने के लिए प्रक्रिया स्थापित की जाएगी और इसके भविष्य में घटने को निवारित करने के लिए अपेक्षित पश्चात्वर्ती कार्य का निर्धारण किया जाएगा । ऐसी प्रक्रिया के अन्तर्गत निम्नलिखित होगा :

- (i) प्रणाली प्रशासक, प्रणाली सुरक्षा प्रशासक और प्रबंध की भूमिका ;
- (ii) अन्वेषण के लिए प्रक्रिया ;
- (iii) सुरक्षा समीक्षा के लिए क्षेत्र ; और
- (iv) प्रश्चात्वर्ती अनुवर्ती कार्य ।

6. प्रणाली की अक्षतता और सुरक्षा उपाय

6.1. सुरक्षा प्रणालियों या सुविधाओं का उपयोग

(1) अप्राधिकृत उपयोगकर्ताओं को सूचना प्रणाली में प्रवेश प्राप्त करने से रोकने के लिए और डाटा में अप्राधिकृत अभिगम के निवारण के लिए प्रत्येक कंप्यूटर प्रणाली या कंप्यूटर नोड पर सुरक्षा नियंत्रण स्थापित और अनुरक्षित किए जाएंगे ।

(2) किसी भी प्रणाली साफ्टवेयर या कंप्यूटर प्रणाली संसाधन में, अभिगम नियंत्रण प्रणाली द्वारा प्राधिकृत किए जाने के पश्चात् ही पहुंच प्राप्त की जानी चाहिए ।

6.2. प्रणाली अभिगम नियंत्रण

(1) अभिगम नियंत्रण साफ्टवेयर और प्रणाली साफ्टवेयर सुरक्षा विशेषताओं को संसाधनों के संरक्षण के लिए कार्यान्वित किया जाएगा । उपयोगकर्ता पहचान और संसाधन विशेषाधिकार जारी करने को प्राधिकृत किए जाने के लिए प्रबंध अनुमोदन अपेक्षित है ।

(2) स्मृति, भंडारण, युक्तियों आदि की तरह के सूचना प्रणाली संसाधनों और संवेदनशील उपयोगिताओं तथा डाटा संसाधनों और कार्यक्रम फाइलों तक अभिगम कर्तव्यों के उचित पृथक्करण के साथ “उपयोग की आवश्यकता” के आधार पर नियंत्रित और निर्बंधित किया जाएगा ।

(3) अभिगम नियंत्रण साफ्टवेयर या कंप्यूटर प्रणाली की प्रचालन प्रणाली उक्त प्रणाली और डाटा संसाधनों तक अभिगम को नियंत्रित करने के लिए रूप रेखा उपबंधित करेगी । प्रणाली और डाटा संसाधनों तक पहुंच को नियंत्रित करने के लिए “एडमिनिस्ट्रेटर” या “प्रेसीडेंट” या “गेम” आदि जैसे सामान्य संकेत शब्दों से सुरक्षा आरक्षित होगी और उनसे बचना चाहिए । सभी संकेत शब्दों को शब्दकोश के हमलों का प्रतिरोधी होना चाहिए ।

(4) प्रणाली संसाधनों तक अभिगम के अनुरोध केतिए उचित अनुमोदन प्रणाली प्रशासक से अभिप्राप्त किया जाएगा । अभिगम प्राधिकारों को शासित करने वाले मार्गदर्शक सिद्धान्त और प्रक्रियाएं विकसित, प्रलेखीकृत और कार्यान्वित की जाएंगी ।

(5) मैनुअल अनुदत्त करने के लिए प्रणाली प्रशासक के मार्गदर्शन के लिए विभिन्न स्तर के उपयोगकर्ताओं को अनुदत्त पहुंच को प्रलेखीकृत करने वाले अभिगम नियंत्रण प्रणाली तैयार किया जाएगा ।

(6) प्रत्येक उपयोगकर्ता को एक विलक्षण उपयोगकर्ता पहचान प्रदान की जाएगी । उपयोगकर्ताओं की संकेत शब्द विकल्प और संकेत शब्द संरक्षण में सहायता करने के लिए पर्याप्त उपयोगकर्ता शिक्षा प्रदान की जाएगी । उपयोगकर्ता के पहचान में हिस्से को अनुज्ञात नहीं किया जाएगा ।

(7) भण्डारित संकेत शब्द, अप्राधिकृत प्रकटन और उपान्तरण को रोकने के लिए अंतरराष्ट्रीय रूप से प्रमाणित तकनीकों का प्रयोग करते हुए गूढ़तेखित किए जाएंगे ।

(8) भण्डारित संकेत शब्दों की अप्राधिकृत प्रकटन और उपान्तरण से अभिगम नियंत्रणों द्वारा संरक्षा की जाएगी ।

(9) टर्मिनल के क्रियाकलापों के लिए स्वचालित टाइम आउट लागू किया जाएगा ।

(10) सुरक्षा संवेदनशील अभिगम के आडिट ट्रेल और किए गए कार्यों का लॉग किया जाएगा ।

(11) आडिट ट्रेल के सभी प्ररूप अप्राधिकृत उपान्तरण या लोप के विरुद्ध समुचित रूप से संरक्षित किए जाएंगे ।

(12) जहां द्वितीय स्तर का अभिगम, नियंत्रण, उपयोजन प्रणाली, द्वारा लागू किए जाते हैं वहां संकेत शब्द जो कंप्यूटर प्रणाली के लिए लागू किए जाने वाले नियंत्रणों के समान हैं, यथावत् होनी चाहिए ।

(13) सभी दूरस्थ उपयोगकर्ताओं के क्रियाकलापों को लॉग किया जाना चाहिए और सावधानीपूर्वक मानिटर करना चाहिए ।

(14) एक उपयोगकर्ता के लाजिन से किसी अन्य उपयोगकर्ता के रूप में लाजिन की सुविधा अनुज्ञात नहीं की जाएगी । तथापि, प्रणाली न्यासित उपयोगकर्ता के रूप में सीधे लाजिन को प्रतिषिद्ध करेगी (उदाहरणार्थ रूट इन यूनिक्स, एडमिनिस्ट्रेटर इन विन्डोज एनटी या विन्डोज, 2000) । इसका अभिप्राय यह है कि न्यासित प्रशासक के पास उपयोगकर्ता का प्रथक् लेखा होना चाहिए । प्रणाली न्यासित उपयोगकर्ता से यह अपेक्षा करती है कि वह रूट में अभिगम प्राप्त करने के लिए उपयोगकर्ता के नाम को बदल दे और विशेषाधिकार प्राप्त कार्यों में अभिगम का अनुरोध करने से पूर्व उन को पुनः प्राधिकृत करे ।

(15) सुरक्षा साफ्टवेयर को शुरू करने और बंद करने की प्रक्रिया स्वचालित होनी चाहिए ।

(16) संवेदनशील प्रचालन प्रणाली फाइलें जो हैकर्स के प्रति अधिक प्रणत हैं, सभी ज्ञात हमलों से प्रमाणित उपकरणों और तकनीकों का प्रयोग करते हुए संरक्षित की जाएंगी, अर्थात् कोई भी उपयोगकर्ता प्रणाली प्रशासक की अनुमति के बिना उनकों उपान्तरित करने के लिए सक्षम नहीं होगी ।

6.3 संकेत शब्द प्रबन्धन

(1) संकेत शब्द के लिए कतिपय न्यूनतम क्वालिटी मानक प्रवृत्त किए जाएंगे । क्वालिटी का स्तर धीरे धीरे बढ़ाया जाएगा । संकेत शब्दों के लिए निम्नलिखित नियंत्रण रूप रेखा कार्यान्वित की जाएंगी :-

- (i) लीडिंग या ट्रेलिंग ब्लैंक्स के बिना न्यूनतम आठ लक्षण ;
- (ii) विद्यमान संकेत शब्द और पूर्ववर्ती दो संकेत शब्दों से भिन्न होंगे ;
- (iii) प्रत्येक नब्बे दिन में कम से कम एक बार बदल दिए जाएंगे ; संवेदनशील प्रणाली के लिए संकेत शब्द प्रत्येक तीस दिन में कम से कम एक बार बदला जाएगा ;
- (iv) किसी के साथ हिस्सा नहीं किया जाएगा, प्रदर्शित या मुद्रित नहीं किया जाएगा ।

(2) संकेत शब्द रिट्रीज अधिकतम तीन अटेम्पट लाग-अन्स तक सीमित होंगी जिसके पश्चात् उपयोगकर्ता की पहचान को प्रतिसंहित कर लिया जाएगा ; संवेदनशील प्रणालियों के लिए संकेत शब्द रिट्रीज की संख्या अधिकतम दो तक सीमित होगी ।

(3) ऐसे संकेत शब्दों से बचा जाए जिनके बारे में अंदाज लगाना आसान है (जैसे उपयोगकर्ता का नाम, जन्म तिथि, मास, मानक शब्द आदि) ।

- (4) आरंभिक और अन्त का संकेत शब्द उपयोगकर्ता द्वारा पहले उपयोग के पश्चात् ही बदल दिया जाना चाहिए ।
- (5) संकेत शब्द अप्राधिकृत प्रकटन को रोकने के लिए भंडारण में हमेशा ही गूढ़लेखित होंगे ।
- (6) सभी प्रयुक्त संकेत शब्द शब्द-कोष प्रहारों के प्रतिरोधी होने चाहिए और सभी ज्ञात संकेत शब्द क्रैकिंग एल्गोरिदम प्रतिरोधी होने चाहिए ।

6.4 विशेषाधिकार प्राप्त उपयोगकर्ता का प्रबंध

- (1) प्रणाली विशेषाधिकार उपयोगकर्ताओं के उपयोग की आवश्यकता के आधार पर ही अनुदत्त किए जाएंगे ।
- (2) अत्यधिक विशेषाधिकार प्राप्त लेखाओं के लिए लाजिन विशेषाधिकार केबल कंसोल या कंसोल कक्ष के भीतर स्थित टर्मिनलों से उपलब्ध होंगे ।
- (3) विशेषाधिकार प्राप्त उपयोगकर्ता द्वारा किए गए आडिट ट्रेल क्रियाकलाप दो वर्ष तक रखे जाएंगे और उनकी ऐसे प्रचालक द्वारा जो प्रणाली प्रशासक से स्वतंत्र है, सावधिक रूप से कम से कम साप्ताहिक समीक्षा की जाएगी ।
- (4) विशेषाधिकार प्राप्त उपयोगकर्ता को कंप्यूटर प्रणाली में दूरस्थ टर्मिनल से लॉग करने के लिए अनुज्ञात नहीं किया जाएगा । विशेषाधिकार प्राप्त उपयोगकर्ता द्वारा कंप्यूटर प्रणाली का उपयोग एक निश्चित समय अवधि के दौरान ही अनुज्ञात किया जाएगा ।
- (5) विशेषाधिकार प्राप्त और सामान्य (जिन्हें विशेषाधिकार प्राप्त नहीं है) क्रियाकलाप करने के लिए उपयोगकर्ता को पृथक उपयोगकर्ता पहचान अनुज्ञात की जाएगी ।
- (6) आपातकालीन उपयोग के लिए उपयोगकर्ता पहचान का उपयोग अभिलिखित और अनुमोदित किया जाएगा । संकेत शब्द उपयोग के पश्चात् मिटा दिए जाएंगे ।

6.5 उपयोगकर्ता का लेखा प्रबंधन

- (1) उपयोजन प्रणाली और डाटा तक अभिगम को नियंत्रित करने के लिए उपयोगकर्ता लेखा प्रबंधन के लिए प्रक्रिया स्थापित की जाएगी । प्रक्रियाओं के अंतर्गत निम्नलिखित होगा :

 - (i) उपयोगकर्ताओं को कंप्यूटर सेवाओं तक अभिगम करने के लिए कंप्यूटर प्रणाली के स्वामी द्वारा प्राधिकृत किया जाएगा ।
 - (ii) अभिगम अधिकारों का एक लिखित कथन सभी उपयोगकर्ताओं को दिया जाएगा ।
 - (iii) सभी उपयोगकर्ताओं से इस अभिस्वीकृति के लिए वचनबंध पर हस्ताक्षर करने की अपेक्षा की जाएगी कि वे अभिगम की शर्तों को समझ रहे हैं ।
 - (iv) जहां कंप्यूटर सेवाओं तक अभिगम का सेवा प्रदाताओं द्वारा प्रशासन किया जाता है वहां यह सुनिश्चित किया जाएगा कि सेवा प्रदाता अभिगम तक तब प्रदान नहीं करते जब तक कि प्राधिकार की प्रक्रियाएं पूरी न कर ली गई हों । इसके अंतर्गत उपयोगकर्ताओं द्वारा लेखाओं की प्राप्ति की अभिस्वीकृति भी है ।
 - (v) कंप्यूटर सेवाओं के सभी रजिस्ट्रीकृत उपयोगकर्ताओं का औपचारिक अभिलेख रखा जाएगा ।
 - (vi) ऐसे उपयोगकर्ताओं के अभिगम अधिकारों को जिनका स्थानान्तरण हो गया है या जिन्होंने संगठन छोड़ दिया है, तत्काल हटा दिया जाएगा ।
 - (vii) अनावश्यक उपयोगकर्ता लेखाओं और ऐसे अभिगम अधिकारों की जिनकी अब आवश्यकता नहीं हैं, सावधिक जांच की जाएगी ।
 - (viii) यह सुनिश्चित करना कि अनावश्यक उपयोगकर्ता लेखा किसी अन्य उपयोगकर्ता को पुनः जारी नहीं किए गए हैं ।

(2) उपयोगकर्ता लेखा निम्नलिखित दशाओं में निलम्बित कर दिए जाएंगे :

- (i) जब कोई व्यष्टि तीस दिन से अधिक के विस्तारित अवकाश पर है या उसका उपयोग निष्क्रिय हो गया है संरक्षित कंप्यूटर प्रणाली की दशा में, तीस दिन की उक्त अवधि को प्रणाली प्रशासक द्वारा घटा कर पन्द्रह दिन किया जा सकेगा ।
- (ii) किसी व्यष्टि की सेवाओं की ठीक समाप्ति पर
- (iii) निलम्बित या निष्क्रिय लेखाओं का दो मास की अवधि के पश्चात् लोप कर दिया जाएगा । संरक्षित कंप्यूटर प्रणालियों की दशा में दो मास की उक्त परिसीमा को घटा कर एक मास किया जा सकेगा ।

6.6 डाटा और साधन संरक्षण

(1) सभी सूचना आस्तियां उस डाटा/साधन की अक्षतता के लिए जिम्मेदार “स्वामी” को समनुदेशित की जाएंगी । संरक्षकों को समनुदेशित की जाएंगी और स्वामियों की सहायता करने के लिए कंप्यूटर नियंत्रण प्रदान करके सूचना आस्तियों के लिए संयुक्त जिम्मेदारी सौंपी जाएगी ।

(2) कंप्यूटर प्रणाली की प्रचालन प्रणाली या सुरक्षा प्रणाली -

- (i) उपयोगकर्ता के प्राधिकार को परिमित करेगी और कंप्यूटर प्रणाली के अंदर डाटा तक पहुंच को नियंत्रित करेगी ;
- (ii) प्रत्येक नामित व्यष्टि के लिए नामित डाटा उद्देश्यों (फाइल, कार्यक्रम की सूची) या नामित उद्देश्यों के समूह और अनुज्ञात पहुंच की किसी को विनिर्दिष्ट करने में सक्षम होगी ।
- (3) नेटवर्क या सम्मिलित कंप्यूटर प्रणालियों के लिए प्रणाली का उपयोग करने वालों को उनके आवश्यक कार्यों को पूरा करने के लिए अपेक्षित डाटा उद्देश्यों के रेखांचित्र तक सीमित किया जाएगा ।
- (4) किसी डाटा और/या साधनों के लिए अभिगम नियंत्रण प्रणाली विश्लेषण और डिजाइन प्रक्रिया के भाग के रूप में अवधारित किए जाएंगे ।
- (5.) उपयोगजन कार्यक्रमक उत्पादन प्रणाली तक पहुंच प्राप्त करने के लिए अनुज्ञात नहीं किए जाएंगे ।

7. संवेदनशील प्रणालियों का संरक्षण

(1) कंप्यूटर प्रणाली में अभिगम के लिए संकेत शब्दों के उपयोग को पूरा करने के लिए सुरक्षा टोकन/स्मार्ट कार्ड/जैव सांख्यिकी प्रौद्योगिकी का जैसे आयरिश मान्यता, अंगुली छाप सत्यापन प्रौद्योगिकियों आदि का उपयोग किया जाएगा ।

(2) कंप्यूटर प्रणाली, प्रसंस्करण संवेदनशील डाटा के लिए अन्य संगठनों द्वारा अभिगम प्रतिषिद्ध किया जाएगा या कठोरता से नियंत्रित किया जाएगा ।

(3) संवेदनशील डाटा के लिए भंडारण में डाटा के गूढ़ लेखन पर उसकी गोपनीयता और विश्वसनीयता की सुरक्षा के लिए विचार किया जाएगा ।

8. डाटा केन्द्र के प्रचालन की सुरक्षा

8.1 कार्य नियतन

(1) यह सुनिश्चित करने के लिए प्रक्रियाएं स्थापित की जाएंगी कि कार्य नियतन के लिए सभी परिवर्तनों का समुचित रूप से अनुमोदन किया जाता है । कार्य नियतन में परिवर्तनों का अनुमोदन करने का प्राधिकार स्पष्टरूप से समनुदेशित किया जाएगा ।

(2) जहां तक संभव हो, स्वचालित कार्य नियतन का प्रयोग किया जाएगा । हस्तचालित कार्य नियतन के लिए सक्षम प्राधिकारी का पूर्व अनुमोदन अपेक्षित होना चाहिए ।

8.2 प्रणाली के प्रचालन की प्रक्रिया

- (1) यह सुनिश्चित करने के लिए प्रक्रियाएं स्थापित की जाएंगी कि केवल प्राधिकृत और सही कार्य धारा और पैरामीटर परिवर्तन किए जाते हैं ।
- (2) प्रणाली क्रियाकलापों के लॉग का अनुस्करण करने के लिए प्रक्रियाएं स्थापित की जाएंगी । ऐसे लॉग की समीक्षा संदिग्ध क्रियाकलापों के उपर्दर्शन के लिए स्वतंत्र पक्षकार द्वारा जाएगी । ऐसे लागों के लिए समुचित प्रतिधारण अवधि समीक्षा की स्थापित की जाएगी ।
- (3) यह सुनिश्चित करने के लिए प्रक्रियाएं स्थापित की जाएंगी कि सुप्रशिक्षित परिचालकों से भिन्न व्यक्ति कंप्यूटर उपस्कर का प्रचालन करने से प्रतिषिद्ध किए जाते हैं ।
- (4) सुरक्षित भण्डारण या सभी उत्पादों/स्प्रिटों के वितरण को सुनिश्चित करने के लिए, प्रत्येक प्रणाली के लिए उसके स्वामियों द्वारा परिभाषित प्रक्रियाओं के अनुसार प्रक्रियाएं कार्यान्वित की जाएंगी ।

8.3 मीडिया प्रबंधन

- (1) मीडिया पुस्तकालय प्रबंधन और संरक्षण के लिए उत्तरदायित्व स्पष्ट रूप से परिभाषित और समनुदेशित किए जाएंगे ।
- (2) ऐसे सभी मीडिया, जिनमें संवेदनशील डाटा हैं, तालाबंद कमरे में या अल्मारियों में भण्डारित किए जाएंगे जो अग्निरोधी और विषेले रसायनों से मुक्त होंगी ।
- (3) मीडिया पुस्तकालय में अभिगम (स्थलीय और अपस्थलीय दोनों तरह के) प्राधिकृत व्यक्तियों तक ही निर्बंधित किया जाएगा । पुस्तकालय में प्रवेश करने के लिए प्राधिकृत कार्मिकों की सूची रखी जाएगी ।
- (4) ऐसे मीडिया, जिनमें संवेदनशील और बैकअप डाटा अन्तर्विष्ट हैं, देश में तीन विभिन्न वस्तुगत स्थानों में भण्डारित किया जाएगा जिस तक केवल कुछ ही घंटों के लिए पहुंचा जा सकेगा ।
- (5) स्थलीय और अपस्थलीय भण्डारित सभी मीडिया के लिए लेखा जोखा रखने के लिए मीडिया प्रबंधन प्रणाली यथावत् होगी ।
- (6) सभी इनकमिंग/आउट गोईंग मीडिया अन्तरण प्रबंधक और उपयोगकर्ताओं द्वारा प्राधिकृत किए जाएंगे ।
- (7) सभी मीडिया की स्वतंत्र वस्तुगत सूची जांच प्रत्येक छह (6) महीने बाद की जाएगी ।
- (8) सभी मीडिया की बाह्य जिल्ड पहचान होगी । आन्तरिक लेबल, जहां भी उपलब्ध हों, लगाए जाएंगे ।
- (9) यह सुनिश्चित करने के लिए प्रक्रियाएं यथावत् होंगी कि पुस्तकालय से मीडिया में केवल प्राधिकृत संकलन/निष्कासन अनुज्ञात किए जाते हैं ।
- (10) मीडिया प्रतिधारण अवधि तय की जाएगी और प्रबंधक द्वारा विधिक/विनियामक और उपयोगकर्ता की उपेक्षाओं के अनुसार, अनुमोदित की जाएगी ।

8.4 मीडिया संचलन

- (1) स्थलीय और अपस्थलीय मीडिया पुस्तकालय के बीच कंप्यूटर टेपों/डिस्कों के सभी संचलनों का उचित अभिलेख रखा जाएगा ।
- (2) बाह्य पक्षकारों और अपस्थलीय अवस्थान को/से मीडिया के प्राधिकृत और सुरक्षित अंतरण को सुनिश्चित करने के लिए प्रक्रियाएं होंगी । प्राप्ति के अधिप्रमाणन के साधन यथावत् होंगे ।
- (3) कंप्यूटर मीडिया, जो अपस्थलीय डाटा बैकअप अवस्थितियों को अन्तरित किए जा रहे हैं, तालाबंद पैटियों में रखे जाएंगे जब उन्हें परिवहन के दौरान लादा और उतारा जा रहा हो चुम्बकीय क्षेत्र संरक्षण और संधात से संरक्षण प्रदान करती होंगी ।

9. डाटा बैकअप और अवस्थालीय प्रतिधारण

- (1) बैकअप प्रक्रियाएं प्रलेखीकृत, अनुसूचित और मानिटर की जाएंगी ।
- (2) सभी नाजुक मदों के अद्यतन बैक अप सेवा के न्यूनतम अनिवार्य स्तर के नियमित उपबंध को सुनिश्चित करने के लिए रखे जाएंगे । इन मदों के अंतर्गत निम्नलिखित हैं -
 - (i) डाटा फाइलें ;
 - (ii) उपयोगिता ओं के कार्यक्रम ;
 - (iii) डाटा बेस ;
 - (iv) प्रचालन प्रणाली साफ्टवेयर ;
 - (v) उपयोजन प्रणाली साफ्टवेयर ;
 - (vi) गूढ़ लेखन कुंजियां ;
 - (vii) पूर्वमुद्रित प्ररूप ; और
 - (viii) प्रलेखन (जिसके अंतर्गत कारबार निरन्तरता योजनाओं की प्रति भी है)
- (3) सभी प्रचालन प्रणाली और उपयोजन साफ्टवेयर के लिए मूल डिस्कों का एक सेट यह सुनिश्चित करने के लिए रखा जाएगा कि वायरस एक विधिमान्य मुक्त बैकअप विद्यमान है और हर समय उपयोग के लिए उपलब्ध हैं ।
- (4) प्रणाली, उपयोजन और डाटा के बैकअप का कार्य नियमित आधार पर किया जाएगा । बैकअप विकास और डाटा संपरिवर्तन के प्रयासों के अधीन उपयोजन के लिए भी किया जाएगा ।
- (5) व्यक्तिगत कंप्यूटरों, सरवरों और वितरण प्रणालियों तथा डाटा बेसों सहित सभी प्रणालियों के लिए डाटा बैकअप अपेक्षित है ।
- (6) नाजुक प्रणाली डाटा और फाइल सरवर साफ्टवेयर को साप्ताहिक रूप से पूर्ण बैकअप मिलना चाहिए ।
- (7) बैकअप ऐसे क्षेत्र में रखा जाना चाहिए जो सरवर से वस्तुगत रूप में पृथक् हो । यदि एल ए एन पर नाजुक डाटा प्रणाली सूचना आस्तियों का विलक्षण रूप प्रस्तुत करती हो तो सूचना बैकअप को अपस्थलीय भण्डारण अवस्थिति पर सावधिक आधार पर चक्रानुगत किया जाएगा ।
- (8) नाजुक डाटा प्रणाली और फाइल सरवर साफ्टवेयर को प्रतिदिन बढ़ी हुई स्थिति में बैकअप मिलना चाहिए ।
- (9) ऐसी प्रणालियों को, जो पूर्णरूप से स्थित हैं, सावधिक बैकअप की आवश्यकता नहीं होती है किन्तु सूचना में परिवर्तनों या अद्यतनों के पश्चात् बैकअप की आवश्यकता होगी ।
- (10) प्रत्येक एल ए एन /प्रणाली के पास कारबार प्रचालनों की निरन्तरता सुनिश्चित करने के लिए प्राथमिक और बैकअप प्रचालक होना चाहिए ।
- (11) कारबार समुत्थान योजना की वार्षिक आधार पर परीक्षा की जानी चाहिए ।

10. संपरीक्षा ट्रेल्स और सत्यापन

- (1) उन संव्यवहारों को, जो आपवादिक मानदंड को पूरा करते हैं, पूर्ण रूप से और समुचित रूप से विशेषीकृत किया और उन कार्मिकों भिन्न कार्मिकों से द्वारा समीक्षा की जाएगी जिन्होंने उस संव्यवहार की शुरूआत की थी ।
- (2) पर्याप्त संपरीक्षा ट्रेल्स संगृहीत किए जाएंगे और संवेदनशील घटनाओं तथा पैटर्न विश्लेषणों का अवधारण करने के लिए आवश्यक कतिपय सूचना का, जो उक्त प्रणाली के संभावित कपटयुक्त उपयोग को उपदर्शित करती है (बारबार असफल लोगोन्स, कई दिनों तक अभिगम के प्रयास), विश्लेषण किया जाएगा । इस सूचना के अंतर्गत ऐसी सूचना भी है जैसे कौन, क्या, कब, कहां और कोई विशेष सूचना जैसे -

(i) उस घटना की सफलता या असफलता ;

(ii) अधिप्रमाणन कुंजियों का उपयोग, जहां लागू होती हैं

(3) सभी महत्वपूर्ण सुरक्षा घटनाओं का मानीटर और उसकी तत्काल रिपोर्ट करने के लिए स्वचालित या हस्तचालित प्रक्रियाओं का उपयोग किया जाना चाहिए जैसे कि ऐसी सफलताएं, जो पैटर्न बाह्य समय से सुसंगत सफलताएं, उनकी मात्रा, आवृत्तियां, सूचना आस्तियों की किस्म और उसकी अत्यधिकता । विश्लेषण के अन्य क्षेत्रों के अन्तर्गत निम्नलिखित हैं :

(i) महत्वपूर्ण कंप्यूटर प्रणाली की घटनाएं (जैसे विन्यास, अद्यतन, प्रणाली क्रेशेस) ;

(ii) सुरक्षा प्रोफाइल परिवर्तन ;

(iii) कंप्यूटर प्रचालकों, प्रणाली प्रशासकों, प्रणाली कार्यक्रमकों और/या सुरक्षा प्रशासकों द्वारा किए गए कार्य ।

(4) कंप्यूटर प्रणाली की वास्तविक समय घड़ी संपरीक्षा लॉग की परिशुद्धता को सुनिश्चित करने के लिए सही रूप से स्थापित की जाएगी जो विधिक या अनुशासनिक मामलों में साक्ष्य के रूप में या अन्वेषण के लिए अपेक्षित हो ।

(5) कंप्यूटर या संसूचना युक्ति की वास्तविक समय घड़ी भारतीय मानक समय (आई एस टी) के अनुसार, स्थापित की जाएगी । इसके अतिरिक्त, एक ऐसी प्रक्रिया भी लगाई जाएगी, जो वास्तविक समय घड़ी की निष्क्रियता को रोकने के लिए और सही करने के लिए होगी ।

(6) कंप्यूटर प्रणाली अभिगम अभिलेख या तो हार्ड कापी या इलेक्ट्रानिक रूप में कम से कम दो 2 वर्ष के लिए रखे जाएंगे । ऐसे अभिलेख, जो विधिक प्रकृति के हैं और किसी विधिक या विनियमन अपेक्षा या आपराधिक आचरण के अन्वेषण के लिए आवश्यक हैं, भारतीय विधि के अनुसार प्रतिधारित किए जाएंगे ।

(7) उपयोजन संव्यवहारों के और महत्वपूर्ण घटनाओं के कंप्यूटर अभिलेख कम से कम दो 2 वर्ष तक या ऐसी लम्बी अवधि तक प्रतिधारित किए जाएंगे जो विनिर्दिष्ट अभिलेख प्रतिधारण अपेक्षाओं पर निर्भर करेगी ।

11. कंप्यूटर वायरस से निपटने के लिए उपाय

(1) यह सुनिश्चित करने के लिए उत्तरदायित्व और कर्तव्य समनुदेशित जाएंगे कि सभी फाइल सरवरों और व्यक्तिगत कंप्यूटरों में अद्यतन संसूचन साफ्टवेयर लगाया गया है ।

(2) वायरस संसूचन साफ्टवेयर का उपयोग प्रणाली में आन्तरिक और बाहरी दोनों ही प्रकार के भण्डारण संचालन की सावधिक आधार पर जांच करने के लिए किया जाएगा ।

(3) सभी डिस्केटों और साफ्टवेयरों का प्रदर्शन किया जाएगा और कंप्यूटर प्रणाली में लोड किए जाने से पूर्व, वायरस संसूचन साफ्टवेयर द्वारा सत्यापन किया जाएगा । बाहर से लॉग किए गए टेप कारतूसों, फ्लापियों आदि की तरह के किसी चुम्बकीय मीडिया का डाटा, फाइल, पी के आई या कंप्यूटर सरवर या व्यक्तिगत कंप्यूटर पर इंट्रानेट और इंटरनेट पर वायरस संसूचन साफ्टवेयर द्वारा उचित प्रदर्शन और सत्यापन के बिना उपयोग नहीं किया जाएगा ।

(4) कंप्यूटर वायरस की प्रतिवेदित या संदेहयुक्त घटनाओं से निपटने के लिए एक दल अभिहित किया जाएगा । अभिहित दल यह सुनिश्चित करेगा कि एन्टी वायरस साफ्टवेयर का नवीनतम संस्करण सभी डाटा, फाइल, पी के आई सरवरों और व्यक्तिगत कंप्यूटरों में लगा दिया गया है ।

(5) अन्य संगठन सूचना आस्तियों में वायरस के फैलने को रोकने के लिए प्रक्रियाएं स्थापित की जाएंगी, ऐसी प्रक्रियाओं में अन्य बातों के साथ-साथ निम्नलिखित सम्मिलित होगा :-

(i) अन्य कारबार भागीदारों और उपयोगकर्ताओं को संसूचना जिन्हें संदूषित साधन से जोखिम हो सकती है ;

(ii) उन्मूलन और समुत्थान प्रक्रियाएं ;

(iii) घटना की रिपोर्ट प्रलेखीकृत की जाएगी और स्थापित प्रक्रियाओं के अनुसार संसूचित की जाएगी ।

(6) वायरस संक्षण पद्धतियों, उपलब्ध नियंत्रणों, वायरस संदूषण के लिए उच्च खतरे के क्षेत्रों और उत्तरदायित्वों के बारे में संसूचना देने के लिए एक जागरूकता और प्रशिक्षण कार्यक्रम स्थापित किया जाएगा ।

12. हार्डवेयर और साफ्टवेयर का पुनर्स्थापन

(1) जब भी कंप्यूटरों या पेरीफरलों को (जैसे विभिन्न स्थलों या भण्डारणों पर रखरखाव, स्थापन) पुनर्स्थापित किया जाए तब निम्नलिखित मार्गदर्शक सिद्धांत लागू होंगे :

- (i) सभी हटाए जाने योग्य मीडिया को कंप्यूटर प्रणाली से हटाया जाएगा और एक सुरक्षित स्थान पर रखा जाएगा ।
- (ii) आंतरिक प्रवृत्तियों को स्थिति के अनुसार, पुन लिखा जाएगा, पुनः प्ररूपित किया जाएगा या हटा लिया जाएगा ।
- (iii) यदि लागू हो तो रिबन प्रिन्टरों से हटा लिए जाएंगे ।
- (iv) प्रिन्टरों से सभी कागज हटा लिए जाएंगे ।

13. हार्डवेयर और साफ्टवेयर का रखरखाव

जब भी कंप्यूटर या कंप्यूटर नेटवर्क का हार्डवेयर या साफ्टवेयर अनुरक्षण किया जा रहा हो तब निम्नलिखित बातों पर विचार किया जाना चाहिए :—

- (1) विद्युत चुम्बकीय निर्गमों के कारण हस्तक्षेप के प्रभाव को कम करने के लिए सूचना प्रौद्योगिकी उपस्कर का उचित नियोजन और स्थापन ।
- (2) हार्डवेयर की सूची और संस्थिति चार्ट का रखरखाव ।
- (3) हार्डवेयर में लगाई गई सुरक्षा व्यक्तियों की पहचान और उनका उपयोग ।
- (4) हार्डवेयर में किए गए और परिवर्तन का प्राधिकरण, प्रलेखीकरण और नियंत्रण ।
- (5) विद्युत और वातानुकूलन सहित सहायक सुविधाओं की पहचान ।
- (6) अविरत विद्युत प्रदाय की व्यवस्था ।
- (7) उपस्कर और सेवाओं का रखरखाव ।
- (8) उनके द्वारा स्थापित और प्रयुक्त कंप्यूटर हार्डवेयर, साफ्टवेयर (प्रणाली और उपयोजन दोनों ही) और फर्मवेयर के रखरखाव के लिए संगठन उचित व्यवस्था करेगा । यह सुनिश्चित करने की जिम्मेदारी प्रचालन स्थल के भारसाधक अधिकारी की होगी कि हार्डवेयर के रखरखाव के लिए वार्षिक संविदा यथावत है ।
- (9) यदि आवश्यक हो तो कंप्यूटर और संसूचना हार्डवेयर, साफ्टवेयर और फर्मवेयर के प्रदाता के साथ संगठन करार करेगा ।
- (10) रखरखाव कार्मिक अप्रकटन के करारों पर हस्ताक्षर करेंगे ।
- (11) सभी हार्डवेयर और साफ्टवेयर के विक्रय, रखरखाव कर्मचारिवृन्द की पहचान उन्हें रखरखाव कार्य शुरू करने से पूर्व की जाएगी ।
- (12) प्रचालन स्थल/कंप्यूटर प्रणाली और नेटवर्क स्थापन कक्ष के भीतर सभी रखरखाव कार्मिकों के साथ संगठन के प्राधिकृत कार्मिक जाएंगे ।
- (13) रखरखाव के पश्चात् अभिवृद्धि त सुरक्षा मैरामीटर जैसे संकेत शब्द, उपयोगकर्ता की पहचान और लेखा बदल दिए जाएंगे या किसी महत्वपूर्ण सुरक्षा के प्रकटन को कम करने के लिए पुनःस्थापित किए जाएंगे ।

(14) यदि कंप्यूटर प्रणाली कंप्यूटर नेटवर्क या उसकी कोई युक्ति रखरखाव करने के परिणामस्वरूप कंप्यूटर वायरसों के लिए भेद्य है तो प्रणाली प्रबंधक या उपयोगकर्ता कंप्यूटर प्रणाली और उसकी युक्तियों तथा रखरखाव के परिणामस्वरूप वायरस से प्रभावित किसी मीडिया की बारीकी से जांच करने के लिए जिम्मेदार हैं।

14. हार्डवेयर और साफ्टवेयर का क्रय और अनुज्ञापन

(1) ऐसे हार्डवेयर और साफ्टवेयर की, जिनके अंतर्गत सुरक्षा अंतर्विष्ट है या जिनका प्रयोग सुरक्षा को प्रभावी करने के लिए किया जाता है और किसी संगठन प्रणाली या नेटवर्क के लिए उपयोग या उसमें हस्तक्षेप के लिए आशयित है, किसी संविदा, क्रय या पट्टे पर हस्ताक्षर करने से पूर्व, इन सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शक सिद्धांतों का पालन करने के लिए सत्यापन किया जाएगा।

(2) ऐसे साफ्टवेयर का, जो सुरक्षा प्रणाली या प्रचालन प्रणाली, अक्षतता विशेषताओं की अनदेखी करने या उपातंरित करने के लिए सक्षम है, यह अवधारण करने के लिए सत्यापन किया जाएगा कि वे इन सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शक सिद्धांतों के अनुरूप हैं। जहां ऐसा अनुपालन संभव नहीं है वहां यह सुनिश्चित करने के लिए प्रक्रियाएं यथावत् होनी चाहिए कि उस साफ्टवेयर का कार्यान्वयन और प्रचालन प्रणाली की सुरक्षा के साथ कोई समझौता नहीं कर रहा है।

(3) भारतीय प्रतिलिप्यधिकार अधिनियम और सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शक सिद्धांतों के अनुपालन को सुनिश्चित करने के लिए प्रणाली साफ्टवेयर (प्रणाली और उपयोजन साफ्टवेयर) के अर्जन और स्थापन की पहचान करने, चयन करने, कार्यान्वयन और नियंत्रित करने के लिए प्रक्रियाएं लगाई जाएंगी।

(4) किसी भी प्रणाली में चाहे वह परीक्षण की हो या उत्पादन की हो, कोई भी ऐसा साफ्टवेयर जानबूझकर लगाना प्रतिषिद्ध है जिसके विनिर्दिष्ट प्रणाली या नेटवर्क पर उपयोग के लिए अनुज्ञा नहीं दी जाएगी।

(5) जब कोई सुनिश्चित अनुज्ञापन करार विद्यमान न हों तब, मूल्यांकन अवधियों के दौरान के सिवाय कोई साफ्टवेयर प्रणाली पर स्थापित नहीं किया जाएगा और उसका उपयोग नहीं किया जाएगा जिसके लिए उपयोगकर्ता ने, मूल्यांकन के अधीन साफ्टवेयर को स्थापित करने या उसका परीक्षण करने के लिए अनुमति प्रलेखित की है।

(6) अवैध रूप से अर्जित या अप्राधिकृत साफ्टवेयर का किसी कंप्यूटर नेटवर्क या डाटा संसूचना उपस्कर पर उपयोग नहीं किया जाएगा। उस दशा में, जिसमें किसी अवैध रूप से अर्जित या अप्राधिकृत साफ्टवेयर का नेटवर्क प्रशासक को पता लगता है, उसे तत्काल हटा दिया जाएगा।

15. प्रणाली साफ्टवेयर

(1) सभी प्रणाली साफ्टवेयर विकल्पों और पैरामीटरों की प्रबंधक द्वारा समीक्षा की जाएगी और उनका अनुमोदन किया जाएगा।

(2) कार्यान्वयन से पूर्व प्रणाली साफ्टवेयर का व्यापक परीक्षण किया जाएगा और इसकी सुरक्षा कार्यप्रणाली की वैधता की जांच की जाएगी।

(3) उपयोगकर्ताओं को कंप्यूटर प्रणाली में पहुंचने से पूर्व, विक्रेता द्वारा प्रदाय किए गए त्रुटियुक्त उपयोगकर्ता की सभी पहचानों का लोप किया जाएगा या संकेत शब्दों को बदल दिया जाएगा।

(4) कंप्यूटर प्रणाली और संसूचना युक्तियों पर स्थापित प्रणाली साफ्टवेयर के संस्करणों को नियमित रूप से अद्यतन किया जाएगा।

(5) प्रणाली साफ्टवेयर में प्रस्तावित सभी परिवर्तनों को प्राधिकृत पक्षकार द्वारा उचित रूप से न्यायोचित रहराया जाएगा और उनका अनुमोदन किया जाएगा।

(6) प्रणाली साफ्टवेयर में सभी परिवर्तनों के लोंग को कायम रखा जाएगा, पूर्णतः प्रलेखीकृत किया जाएगा और वांछित परिणामों को सुनिश्चित करने के लिए उनकी परीक्षा की जाएगी।

(7) विक्रेताओं द्वारा आरम्भ किए गए नियंत्रण परिवर्तनों की प्रक्रियाएं “परिवर्तन प्रबंधन” से संबंधित पैरा 21 के अनुसार होंगी ।

(8) प्रणाली पुरस्तकालयों में कोई भी स्थायी “राईट” अभिगम नहीं होगा । सभी “राईट” अभिगम लॉग किए जाएंगे और संदिग्ध क्रियाकलापों के लिए प्रणाली प्रशासक द्वारा उनकी समीक्षा की जाएगी ।

(9) उत्पादन पर्यावरण में उपयोजन प्रणाली डाटा और कार्यक्रम फाइलों में अभिगम प्राप्त करने के लिए प्रणाली कार्यक्रमों को अनुज्ञात नहीं किया जाएगा ।

(10) ऐसी संवेदनशील प्रणाली उपयोगिताओं और प्रणाली कार्यक्रमों के, जो आशयित सुरक्षा नियंत्रणों की अनदेखी कर सकते हैं, उपयोग पर नियंत्रण के लिए प्रक्रियाएं यथावत् होंगी और प्रलेखीकृत की जाएंगी । सभी पद्धतियां प्रणाली प्रशासक द्वारा लॉग कर दी जाएंगी और संदिग्ध क्रियाकलापों के लिए प्रणाली प्रशासक से भिन्न किसी व्यक्ति द्वारा भी लॉग की जाएंगी ।

16. प्रलेखन सुरक्षा

(1) उपयोजन साफ्टवेयर और संवेदनशील प्रणाली साफ्टवेयर और उनमें किए गए परिवर्तनों से संबंधित सभी दस्तावेज तत्समय तक अद्यतन रखे जाएंगे और ठीक-ठाक और सुरक्षित भंडारित रखे जाएंगे । सभी प्रलेखनों की अद्यतन तालिका सूची नियंत्रण और जवाबदेही को सुनिश्चित करने के लिए रखी जाएगी ।

(2) सभी प्रलेखनों और पश्चात्वर्ती परिवर्तनों की, जारी करने से पूर्व किसी निष्पक्ष प्राधिकृत पक्षकार द्वारा समीक्षा और अनुमोदन किया जाएगा ।

(3) उपयोजन प्रणाली प्रलेखन और संवेदनशील प्रणाली साफ्टवेयर प्रलेखन पर अभिगम केवल “उपयोग की आवश्यकता” के आधार पर प्राधिकृत कार्मिकों के लिए सीमित रखा जाएगा ।

(4) सभी प्रलेखनों के पर्याप्त बैकअप रखे जाएंगे और सभी नाजुक प्रलेखनों और मैनुअलों की प्रति अवरक्षण पर भंडारित की जाएगी ।

(5) प्रलेखन को उसकी अंतर्वस्तु/उपयोजनों की संवेदनशीलता के अनुसार, वर्गीकृत किया जाएगा ।

(6) संगठनों को प्राधिकृत अभिगम, सामान्य काम के घंटों के बाहर सूचना की हानि या क्षति के खतरे को कम करने के लिए कागजों, डिस्केटों और अन्य प्रलेखन के लिए मेज साफ की नीति अपनानी होगी ।

17. नेटवर्क संसूचना सुरक्षा

(1) नेटवर्क पर सभी संवेदनशील सूचना समुचित तकनीकों का उपयोग करते हुए, संरक्षित की जाएगी । रुटर्स, स्विचों और माडेम्स जैसी नाजुक नेटवर्क युक्तियों की वस्तुगत क्षति से रक्षा की जानी चाहिए ।

(2) नेटवर्क संस्थिति और सूचियों को प्रलेखीकृत किया जाएगा और अनुरक्षित रखा जाएगा ।

(3) नेटवर्क संस्थिति में कोई परिवर्तन करने के लिए नेटवर्क प्रशासक का पूर्व प्राधिकार प्राप्त करना होगा । नेटवर्क संस्थिति में किए गए परिवर्तनों को प्रलेखीकृत किया जाएगा । नेटवर्क संस्थिति में परिवर्तनों के पश्चात् नेटवर्क को खतरे और जोखिम के निर्धारण की समीक्षा की जाएगी । किसी भी सुरक्षा अनियमितता के लिए नेटवर्क प्रचालन की मानीटरी की जाएगी । सुरक्षा समस्याओं की पहचान करने और उनको हल करने के लिए सामान्य प्रक्रियाएं यथावत् होनी चाहिए ।

(4) संसूचना और नेटवर्क स्थलों पर वस्तुगत अभिगम “वस्तुगत अभिगम” से संबंधित पैरा 4.4 के अनुसार, केवल प्राधिकृत व्यक्तियों तक ही नियंत्रित और निर्बंधित किया जाएगा ।

(5) संसूचना और नेटवर्क प्रणालियां पैरा 6.2 - प्रणाली अभिगम नियंत्रण के अनुसार, केवल प्राधिकृत व्यक्तियों तक नियंत्रित और निर्बंधित की जाएगी ।

(6) जहां तक संभव हो, प्रमाणक प्राधिकारी के प्रचालन स्थल के भीतर पारेषण माध्यम को विद्युत चुम्बकीय पारेषण से सुरक्षित रखना चाहिए। इस संबंध में, पारेषण भीड़िया के रूप में, यथास्थिति, आप्टिकल फाइबर केबल और आर्मर्ड केबल के उपयोग को अधिमानता दी जा सकेगी।

(7) नेटवर्क निदान उपकरणों का जैसे वर्णक्रम विश्लेषक, संलेख विश्लेषक का आवश्यकता के आधार पर उपयोग किया जाना चाहिए।

18. फायरवाल्स

(1) संगठन के डाटा नेटवर्क को बाहरी नेटवर्क से अलग करने के लिए अभिज्ञ युक्तियों का, जिन्हें सामान्यतः 'फायरवाल्स' के रूप में जाना जाता है, प्रयोग किया जाना चाहिए। अप्राधिकृत उपयोग के लिए नेटवर्क की संयोजकता को सीमित करने के लिए फायरवाल युक्ति का उपयोग करना चाहिए।

(2) ऐसे नेटवर्क को, जो विभिन्न तुरंत स्तरों पर प्रचालित होते हैं, समुचित फायरवाल द्वारा अन्य नेटवर्कों से अलग किया जाएगा। संगठन के आंतरिक नेटवर्क को इंटरनेट से या किसी अन्य बाहरी संयोजन से वस्तुतः और तर्क्युक्त रूप से अलग करने के लिए फायरवाल का प्रयोग किया जाएगा।

(3) सभी फायरवालों को, उनका उपयोग करने से पूर्व भेद्यता के लिए परीक्षण और उसके पश्चात् छमाही रूप से परीक्षण के अधीन गुजरना होगा।

(4) इंटरनेट उपयोगकर्ताओं द्वारा अभिगम के लिए सभी वैध सरवरों को अन्य डाटा और परिणीषी सरवरों से अलग किया जाएगा।

19. संयोजकता

(1) संगठन अपने कंप्यूटर नेटवर्क या कंप्यूटर प्रणाली को गैर-संगठन कंप्यूटर प्रणाली या नेटवर्क से संबंध जोड़ने के लिए अनुज्ञात करने हेतु प्रक्रिया स्थापित करेगा। अन्य नेटवर्क और कंप्यूटर प्रणाली को जोड़ने की अनुमति का नेटवर्क प्रशासक द्वारा अनुमोदन और प्रलेखीकरण किया जाएगा।

(2) सभी अप्रयुक्त संयोजनों और नेटवर्क सेगमेंटों को सक्रिय नेटवर्क से काट दिया जाना चाहिए। संगठन की होस्ट प्रणाली में अभिगम करने के लिए कंप्यूटर प्रणाली/व्यक्तिगत कंप्यूटर या बाहरी टर्मिनलों को साधारण प्रणाली सुरक्षा और अभिगम नियंत्रण मार्गदर्शनों का पालन करना होगा।

(3) नए हार्डवेयर/सफ्टवेयर विशेषकर प्रॉटोकल प्रतियोगी उपयोगिता का उसे संगठन के नेटवर्क से जोड़ने से पहले निर्धारण किया जाना चाहिए।

(4) जहां तक संभव हो, डाटाबेस सरवर/फाइल सरवर या सरवर होस्टिंग संवेदनशील डाटा में कोई भी इंटरनेट अभिगम अनुज्ञात नहीं किया जाना चाहिए।

(5) संसूचना और नेटवर्क संसाधनों के लिए संरक्षण का स्तर डाटा की नाजुकता और संवेदनशीलता के अनुरूप होगा।

20. नेटवर्क प्रशासक

(1) प्रत्येक संगठन उचित रूप से प्रशिक्षित "नेटवर्क प्रशासक" को पदाभिहित करेगा जो नेटवर्क के प्रचालन, मानीटरी और प्रशासन के लिए जिम्मेदार होगा।

(2) नेटवर्क प्रशासक नेटवर्क की नियमित रूप से समीक्षा करेगा और उसकी सुरक्षा के लिए वस्तुगत, तर्कसंगत और प्रक्रियात्मक रूपोंपाय उपलब्ध कराने के लिए पर्याप्त उपाय करेगा। कंप्यूटर नेटवर्क पर असामान्य क्रियाकलाप या अभिगम किसी पैटर्न के अनुवर्ती कार्य का नेटवर्क प्रशासक द्वारा तत्प्रता से अन्वेषण किया जाएगा।

(3) प्रणाली के अंतर्गत सुरक्षा में संभावित अंगों जैसे अप्राधिकृत अभिगम, वायरस संक्रामण और हैकिंग के लिए नेटवर्क प्रशासक को बदलने के लिए तंत्र भी सम्मिलित हैं।

(4) कंप्यूटर नेटवर्क के कार्यकरण की मानीटरी करने के लिए सुरक्षित नेटवर्क प्रबंधन प्रणाली लागू की जानी चाहिए। नेटवर्क ट्रैफिक का प्रसारण कम से कम किया जाना चाहिए।

(5) नेटवर्क पर केवल प्राधिकृत और वैध साफ्टवेयर का उपयोग किया जाएगा।

(6) कारबार उपयोजन के लिए प्रयोग की गई साझा कंप्यूटर प्रणालियों और नेटवर्क युक्तियों को पैरा 6 - प्रणाली अक्षतता और सुरक्षा नियंत्रण में स्थापित अपेक्षाओं का पालन करना चाहिए।

21. परिवर्तन प्रबंधन

21.1 परिवर्तन नियंत्रण

(1) उत्पादन प्रणाली में उपयोजन साफ्टवेयर, साफ्टवेयर, हार्डवेयर और डाटा में परिभारण और प्रबंध के लिए प्रक्रिया स्थापित की जाएगी। परिवर्तन प्रबंध प्रक्रिया के लिए संगठनात्मक उत्तरदायित्व परिभाषित और समनुदेशित किया जाएगा।

(2) एक जोखिम और प्रभाव विश्लेषण, वर्गीकरण तथा पूर्विकताकरण प्रक्रिया स्थापित की जाएगी।

(3) उत्पादन प्रणाली में कोई परिवर्तन तब तक नहीं किया जाएगा जब तक ऐसे परिवर्तनों का औपचारिक रूप से प्राधिकृत नहीं कर दिया गया है। परिवर्तन नियंत्रण के लिए प्राधिकृत करने की प्रक्रिया को परिभाषित और प्रलेखीकृत किया जाएगा।

(4) स्वामियों और उपयोक्ताओं को उत्पादन प्रणाली में किए गए सभी परिवर्तन अधिसूचित किए जाएंगे जो उक्त उत्पादन पर सूचना के प्रसंस्करण पर प्रभाव डाल सकते हैं।

(5) परिवर्तन प्रक्रिया के कार्यान्वयन में असफलता की दशा में, फाल बैक प्रक्रिया स्थापित और प्रलेखीकृत की जाएगी।

(6) उत्पादन स्रोत कोड, डाटा, निष्पादन विवरणों और सुसंगत प्रणाली प्रलेखीकरण के संरक्षण, नियंत्रण पहुंच तथा उत्पादन के लिए परिवर्तन के लिए प्रक्रिया प्रलेखीकृत तथा कार्यान्वित की जाएगी।

(7) कंप्यूटर प्रणाली प्रतिष्ठापित उपयोग साफ्टवेयर और सभी प्रणाली साफ्टवेयर तथा सभी संसूचना युक्तियों के कथन परिवर्तनों को प्रलेखीकृत किया जाएगा। उपयोग साफ्टवेयर और प्रणाली साफ्टवेयर के विभिन्न कथनों को निश्चित रूप से सुरक्षित अभिरक्षा में रखा जाना चाहिए।

21.2. उत्पादन प्रणाली के लिए परिवर्तनों का परीक्षण

(1) उत्पादन प्रणाली में प्रस्तावित कंप्यूटर संसाधन में सभी परिवर्तनों का परीक्षण किया जाएगा और कार्यान्वयन के पहले सभी संबंधित पक्षकारों द्वारा परीक्षण परिणामों का पुनर्विलोकन किया जाएगा और अभिस्वीकृत किया जाएगा।

(2) उत्पादन प्रणाली में कंप्यूटर संसाधन की बाबत सभी उपयोक्ता अभिस्वीकृति परीक्षण नियंत्रित पर्यावरण में किए जाएंगे जिसके अंतर्गत (i) परीक्षण का उद्देश्य, (ii) एक प्रलेखीकृत परीक्षण योजना, और (iii) स्वीकृत किए जाने का मानदंड भी है।

21.3. परिवर्तन का पुनर्विलोकन

(1) कार्यक्रम परिवर्तनों के उनके उत्पादन पर्यावरण में चले जाने से पूर्व अप्राधिकृत या दोषपूर्ण कोड का पता लगाने के लिए स्वतंत्र पुनर्विलोकन के लिए प्रक्रिया स्थापित की जानी चाहिए।

(2) उत्पादन प्रणाली में कंप्यूटर संसाधन में परिवर्तनों अनुसूचित और पुनर्विलोकन के लिए प्रक्रिया स्थापित की जाएगी जिससे कि उचित कार्यकरण सुनिश्चित किया जा सके।

(3) उत्पादन प्रणाली में कंप्यूटर संसाधन में सभी आपातकालीन परिवर्तन/स्थिरीकरण का पुनर्विलोकन और अनुसोदन किया जाएगा ।

(4) उत्पादन प्रणाली में कंप्यूटर संसाधन में क्रियान्वित परिवर्तनों की प्रास्थिति पर नियतकालिक प्रबंध रिपोर्ट प्रबंध पुनर्विलोकन के लिए प्रस्तुत की जाएगी ।

22. समस्या प्रबंधन और रिपोर्टिंग

(1) समस्याओं का पता लगाने, रिपोर्ट करने और समाधान के लिए जैसे प्रमाणन प्राधिकारी की प्रणाली का काम न करना ; सूचना प्रौद्योगिकी प्रणाली में खामियां तथा वैकिंग प्रक्रिया स्थापित की जाएगी और सभी संबंधित कार्मिकों को संसूचित की जाएगी । इसके अंतर्गत आपातकालीन तीव्रीकरण (इस्केलेशन) प्रक्रिया होगी । प्रबंध के पुनर्विलोकन के लिए नियतकालिक रिपोर्ट प्रस्तुत की जाएगी ।

(2) समस्याओं का निराकरण करने में उपयोक्ताओं की सहायता के लिए एक सहायता डेर्स्क स्थापित की जाएगी ।

(3) रिपोर्ट की गई समस्याओं की प्रास्थिति के अभिलेखन, पथ निर्धारण और रिपोर्ट करने के लिए एक प्रणाली यह सुनिश्चित करने के लिए स्थापित की जाएगी कि उन्हें संगणना संसाधन के उपयोक्ता पर कम से कम प्रभाव के साथ तत्परता से प्रबंधित और निराकृत किया जा सके ।

23. आपातकालीन तैयारी

(1) कंप्यूटर प्रचालन से संबंधित सभी क्रियाकलापों के लिए आपातकालीन प्रतिक्रिया प्रक्रिया विकसित और प्रलेखीकृत की जाएगी ।

(2) आपातकालीन अभ्यास नियतकालिक रूप से यह सुनिश्चित करने की दृष्टि से कराया जाना चाहिए कि प्रलेखीकृत आपातकालीन प्रक्रिया प्रभावी है ।

24. आकस्मिकता प्रत्युद्धरण उपस्कर और सेवाएं

(1) कंप्यूटर उपस्कर और प्रदाय विक्रेताओं से संगणना सुविधा के नष्ट हो जाने पर विनिर्दिष्ट समयावधि के भीतर नाजुक उपस्कर और प्रदाय को बदलने के लिए लिखित रूप में वचनबद्धता अभिप्राप्त की जाएगी ।

(2) कारबार निरंतरता योजना का विकास किया जाएगा जिसके अंतर्गत अन्य बातों के साथ, उपकरण के आपातकालीन आदेश देने के लिए तथा सेवा की उपलभ्यता के लिए प्रक्रिया होगी ।

(3) बैंकअप हार्डवेयर और अन्य परियोगीय (पेरिफेरल्स) के लिए आवश्यकता का कारबार की आवश्यकता के अनुसार मूल्यांकन किया जाना चाहिए ।

25. सुरक्षा घटना का रिपोर्ट किया जाना तथा प्रतिक्रिया

(1) सभी सुरक्षा संबंधी घटनाओं की रिपोर्ट घटनाओं संबंधी सुरक्षा का समन्वय करने और उनको निपटाने के लिए प्रबंध द्वारा नियुक्त केन्द्रीय समन्वयक को की जाएगी । यह केन्द्रीय समन्वयक संगठन में संपर्क का एकल बिन्दु होगा ।

(2) रिपोर्ट की गई सभी घटना, की गई कार्रवाइयां, अनुवर्ती कार्रवाइयों और अन्य संभावित जानकारी प्रलेखीकृत की जाएगी ।

(3) सुरक्षा संबंधी सभी घटनाओं के बारे में, जिसके अंतर्गत द्वेषपूर्ण साफ्टवेयर, नेटवर्कों से भेदन (ब्रेक इन) करने, साफ्टवेयर कीड़ा (बग) जिसने प्रणाली के सुरक्षा को संकट में डाल दिया था, काथरी के लिए प्रक्रिया परिभाषित की जाएगी ।

26. आपदा प्रत्युद्धरण/प्रबंध

(1) आपदा प्रत्युद्धरण योजना विकसित की जाएगी, समुचित रूप से प्रलेखीकृत की जाएगी, परीक्षित की जाएगी और यह सुनियोजित करने के लिए अनुरक्षित की जाएगी कि सूचना प्रणाली के असफल होने या सुविधा के नष्ट हो जाने की दशा में, सेवा को अत्यावश्यक स्तर पर उपलब्ध कराया जा सके । आपदा प्रत्युद्धरण ढांचे में निम्नलिखित होंगे ।

(क) आपातकालीन प्रक्रिया, जिसमें बड़ी घटना की दशा में तत्काल की जाने वाली कार्रवाई का वर्णन किया जाए ।

(ख) फालबंक प्रक्रिया जिसमें अत्यावश्यक क्रियाकलापों या समर्थन सेवाओं को प्रोत्साहन स्थल तक पुनः जमाने के लिए की जानेवाली कार्रवाई का वर्णन हो ।

(ग) प्रत्यावर्तन प्रक्रिया जिसमें मूल स्थल पर सामान्य प्रचालन को बहाल करने के लिए की जाने वाली कार्रवाई का वर्णन हो ।

(2) प्रलेखीकरण के अंतर्गत निम्नलिखित होंगे :—

(क) आपदा की परिभाषा ;

(ख) योजना को क्रियान्वित करने की शर्त ;

(ग) संकट के प्रक्रम ;

(घ) संकट में कौन निर्णय करेगा ;

(ड) योजना के प्रत्येक घटक के लिए व्यष्टियों की भूमिका ;

(च) प्रत्युद्धरण टीम की संरचना ; और

(छ) सामान्य प्रचालन बहाल करने के लिए प्रक्रिया बनाने का निर्णय ।

(3) नाजुक उपयोजनों के लिए विनिर्दिष्ट आपदा प्रबंध योजना विकसित की जाएगी, परीक्षित की जाएगी और नियमित आधार पर बनाई रखी जाएगी ।

(4) उत्तरदायित्व और रिपोर्टिंग संरचना स्पष्ट रूप से परिभाषित की जाएगी जो आपदा की घोषणा पर तत्काल प्रभावी हो जाएगी ।

(5) योजना का प्रत्येक संघटक/पहलु के लिए एक व्यक्ति होना चाहिए और उसके निष्पादन के लिए समनुदेशित बैंकअप होना चाहिए ।

(6) सूचना प्रौद्योगिकी कार्मिक और उपयोक्ताओं का नियतकालिक प्रशिक्षण चलाया जाना चाहिए जिसमें आपदा की दशा में, उनकी भूमिका और उत्तरदायित्व परिभाषित किया जाए ।

(7) परीक्षण योजना विकसित की जाएगी, प्रलेखीकृत की जाएगी और अनुरक्षित की जाएगी । योजना में प्रक्रिया की प्रभाविकता का परीक्षण करने के लिए नियतकालिक परीक्षण किए जाएंगे । परीक्षणों का परिणाम प्रबंध के पुनर्निर्विलोकन के लिए प्रलेखीकृत किया जाएगा ।

(8) आपदा प्रत्युद्धरण योजना को उसकी निरंतर प्रभाविकता सुनिश्चित करने के लिए नियमित रूप से अद्यतन बनाए रखा जाना चाहिए ।

अनुचूची-3
 [नियम 19(2) देखिए]

प्रमाणकर्ता प्राधिकारियों के लिए मार्गदर्शन

अनुक्रमाणिका

	<u>पृष्ठ</u>
1. प्रस्तावना	44
2. सुरक्षा प्रबंध	44
3. वस्तुगत नियंत्रण - रथल अविभिति, सन्तर्माण और वस्तुगत नुस्खा	44
4. मोडिया भारण	45
5. अपशिष्ट व्ययन	46
6. रथल बाह्य बैंक अप	46
7. परिवर्तन और आकृति प्रबंधन	46
8. नेटवर्क और संसूचना सुरक्षा	46
9. प्रणाली सुरक्षा आडिट प्रक्रिया	47
9.1 अभिलिखित धटना का प्रकार	47
9.2 आडिट लाग मानीटरिंग को आवृत्ति	48
9.3 आडिट लाग के लिए प्रतिधारण अवधि	48
9.4 आडिट लाग का संरक्षण	49
9.5 आडिट लाग बैंक अप प्रक्रिया	49
9.6 भेद्यता अवधारण	49
10. अभिलेख आगार	49
11. संकट और विनाश प्रत्युद्धरण	49
11.1 संगणक संसाधन साप्टवेयर और/या डाटा दूषित हैं	49
11.2 प्राकृतिक या अन्य प्रकार के विनाश के पश्चात् सुरक्षा सुनिश्चित करना	49
11.3 आनुबंधिक प्रबंध योजना	50
12. प्रत्येक कार्य के लिए अपेक्षित व्यक्तियों की संख्या	50
13. प्रत्येक भूमिका के लिए पहचान तथा अधिप्रमाणन	50
14. कार्मिक सुरक्षा नियंत्रण	51
15. प्रशिक्षण अपेक्षाएं	51
16. प्रतिधारण भेद्यता और अपेक्षाएं	51
17. कार्मिकों को प्रदाय किए गए प्रलेख	52
18. कुंजी प्रबंध	52
18.1 उत्पादन	52
18.2 कुंजियों का वितरण	52

18.3 भंडारण	52
18.4 उपयोग	52
18.5 प्रमाणकर्ता प्राधिकारी का उपयोक्ता को लागू कुंजी परिवान	52
19. प्राइवेट कुंजी सुरक्षा और बैंक अप	52
20. प्राइवेट कुंजी नष्ट करने की प्रद्वति	53
21. लोक और प्राइवेट कुंजियों के लिए उपयोग अवधि	53
21.1 कुंजी परिवर्तन	53
21.2 नष्ट करना	53
21.3 कुंजी संकट	53
22. हस्ताक्षरकर्ता की सूचना की गोपनीयता ।	54

प्रमाणकर्ता प्राधिकारियों के लिए सुरक्षा मार्गदर्शन

1. प्रस्तावना

यह दस्तावेज प्रबंध और प्रमाणकर्ता प्राधिकारियों के प्रचालन के लिए सुरक्षा मार्गदर्शन विहित करती है और इसका लक्ष्य उनकी सेवाओं, डाटा और प्रणालियों की समग्रता, गोपनीयता और उपलब्धता का संरक्षण करना है । ये मार्गदर्शक प्रमाणकर्ता प्राधिकारी को लागू होते हैं जो अंकीय चिन्हक प्रमाणपत्र के प्रबंध से सहबद्ध सभी कृत्यों का पालन करता है अर्थात् :-

1. रजिस्ट्रीकरण का सत्यापन निदेशन और प्रतिसंहरण अनुरोध
2. अंकीय चिन्हन प्रमाणपत्र का उत्पादन, जारी किया जाना, और प्रतिसंहरण, और
3. अंकीय चिन्हन प्रमाणपत्र का प्रकाशन और अभिलेखाकरण, सूचना का निलंबन और प्रतिसंहरण ।

2. सुरक्षा प्रबंध

प्रमाणकर्ता प्राधिकारी सूचना प्रौद्योगिकी अनुसूची-2 और अनुसूची-3 में परिभाषित आधार पर इसके प्रचालन के लिए सुरक्षानीति परिभाषित करेगा । नीति को सभी कार्मिकों को संसूचित किया जाएगा और उसे संपूर्ण संगठन में सहसुनिश्चित करने के लिए व्यापक रूप से प्रकाशित किया जाएगा कि कार्मिक नीतियों का पालन करें ।

3. वस्तुगत नियंत्रण-स्थल अवस्थिति, संरचना और वस्तुगत पहुंच

(1) प्रमाणकर्ता प्राधिकारी के प्रचालन स्थल की स्थल अवस्थिति, परिकल्पना सन्निर्माण, वस्तुगत और प्रचालन सुरक्षा अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शन सिद्धांत की पैरा 4 के अनुसार होगी ।

(2) उस प्रचालन स्थल तक जिसमें कंप्यूटर वितरक (सर्वर) पी के आई वितरक (सर्वर) संसूचना और नेटवर्क युक्तियां रखी गई हैं, पहुंच अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्ग दर्शक सिद्धांत की पैरा 4.4 के अनुसार नियंत्रित और केवल प्राधिकृत व्यक्तियों तक निर्बंधित रहेगी ।

(3) प्रमाणकर्ता अधिकारी को

- (i) यह सुनिश्चित करना चाहिए कि प्रमाणन स्थल जिसमें पी के आई वितरक (सर्वर, अनुसूचन) और नेटवर्क रखे हैं, अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्ग दर्शक सिद्धांत की अनुसूची 4.2 के अनुसार अग्नि शमन प्रणाली से संरक्षित है ।
- (ii) सुनिश्चित करना चाहिए कि विद्युत और वातानुकूलन नियंत्रण सुविधाएं अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्ग दर्शन सिद्धांतों की अनुसूची 4.1 के अनुसार स्थापित की गई है ।
- (iii) सुनिश्चित करना चाहिए कि सभी हटाने योग्य मीडिया और कागज जिसमें संवेदनशील या

साधारण पाठ सूचना है तथा सूचीबद्ध किए गए हैं तथा प्रलेखीकृत किए गए हैं तथा उचित रूप से पहचान किए गए हैं अधान में भंडारित किए जाते हैं ।

- (iv) सुनिश्चित करना चाहिए कि प्रमाणकर्ता प्राधिकारी के वितरक(सर्वर) तक अनुरक्षित पहुंच उन कार्मिकों तक सीमित है जो किसी पहुंच सूची में पहचान किए गए हैं ।
- (v) सुनिश्चित करना चाहिए कि वास्तविक अंकीय चिन्हांकन प्रणाली की सार्वजनिक रूप से पहचान नहीं की जाएगी ।
- (vi) सुनिश्चित करना चाहिए कि अंकीय चिन्हांकन प्रणाली तक नियन्त्रण और आडिट पहुंच के लिए पहुंच सुरक्षा प्रणाली स्थापित की जाती है ।
- (vii) सुनिश्चित करना चाहिए कि तालिका पर दुहरा नियन्त्रण है और अभिगम कार्ड कुंजियां स्थान पर हैं ।
- (viii) सुनिश्चित करना चाहिए कि उन कार्मिकों की जो अभिगम कार्ड /कुंजियों का कब्जा रखते हों, अद्यतन सूची प्रमाणकर्ता प्राधिकारी के प्रचालन स्थल पर रखी जाती है ।
- (ix) सुनिश्चित करना चाहिए कि ऐसे कार्मिकों के जो अभिगम सूची पर नहीं हैं, साथ उचित रूप से अनुरक्षक रहते हैं और उनका पर्यवेक्षण किया जाता है ।
- (x) सुनिश्चित करना चाहिए कि प्रमाणकर्ता प्राधिकारी के प्रचालन स्थल पर पहुंच लाग रखा जाता है और उसका नियतकालिक निरीक्षण किया जाता है ।

(4) बहु-पर्याय पहुंच तंत्र प्रमाणकर्ता प्राधिकारी के प्रचालन स्थल पर स्थापित किया जाना चाहिए । इस सुविधा में स्पष्ट रूप से इसकी सुविधा के भीतर सुरक्षा क्षेत्र बनाया जाना चाहिए जिसका प्रत्येक सुरक्षा क्षेत्र तक पहुंच आधिकार स्पष्ट रूप परिभासित होना चाहिए । प्रत्येक सुरक्षित क्षेत्र दूसरे से तल से पृथक् होना चाहिए जिसकी छत के भीतर कंकरीट की प्रबलित दीवाल होनी चाहिए । अलार्म तथा अनधिकार प्रवेश पता लगाने की प्रणाली प्रत्येक स्तर पर स्थापित की जानी चाहिए जिसमें पर्याप्त विद्युत बैंक अप हो जिससे मुख्य विद्युत की हानि की दशा में भी प्रचालन जारी रहे । बाह्य सुरक्षा आलर्म मानीटरिंग सेवा (यदि प्रयुक्त की जाती है) के विद्युत/ इलैक्ट्रानिक सर्किट का पर्यवेक्षण किया जाना चाहिए । किसी अकेले व्यक्ति की पी के आई सर्वर, रुट कुंजी या किसी कंप्यूटर प्रणाली या नेटवर्क युक्ति तक स्वयं अपने से पूर्ण पहुंच नहीं होनी चाहिए ।

(5) मुख्य भवन में जहां प्रमाणकर्ता प्राधिकारी की सुविधाएं जैसे डाटा केंद्र पी के आई सर्वर और नेटवर्क युक्तियां धर में रखी गई हैं । प्रवेश तथा प्रत्येक सुरक्षा क्षेत्र में प्रवेश का दिन रात बीड़ियों अभिलेखन किया जाना चाहिए । इस अभिलेख की सावधानी पूर्वक संवीक्षा की जानी चाहिए तथा कम से कम एक वर्ष तक इस अनुरक्षित किया जाना चाहिए ।

(6) प्रमाणकर्ता प्राधिकारी स्थल का अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शन सिद्धांतों के अनुसार सभी समय पर अप्राधिकृत अतिक्रमण के लिए शारीरिक रूप से या इलैक्ट्रानिक रूप से मानिटर किया जाना चाहिए ।

(7) कंप्यूटर प्रणाली/ पी के आई सर्वर जो अंकीय चिह्नक प्रमाणपत्र का कार्य करता है, एक समर्पित कमरे या विभाजन में अवस्थित होगा जिससे वस्तुगत पहुंच नियन्त्रण के प्रवर्तन को सुगम बनाया जा सके । उक्त कमरे या विभाजन का प्रवेश और निर्गम समय स्टांपों सहित स्वचालित ताला से बन्द होंगे और सुरक्षा प्रशासक द्वारा प्रतिदिन पुनर्विलोकन किया जाएगा ।

(8) प्रमाणकर्ता प्राधिकारी प्रणाली के कार्य करने के लिए अत्यावश्यक अवसंरचना घटक तक पहुंच जैसे विद्युत नियन्त्रण पैनेल, संसूचना अवसंरचना, अंकीय चिन्हन प्रमाणन प्रणाली, केबल लगाना आदि प्राधिकृत कार्मिकों तक निर्बंधित होंगे ।

(9) सामान्य वस्तुगत सुरक्षा इंतजाम का पास द्वारा या पुनःप्रेरण प्राधिकृत किया जाएगा और सुरक्षाकार्मिकों द्वारा प्रलेखीकृत किया जाएगा ।

(10) कार्यालय समय के दौरान और उसके पश्चात् अंकीय चिन्हक प्रमाणन प्रणाली तक वस्तुगत पहुंच मानीटर करने और अभिलिखित करने के लिए अधिक्रमण खोजी प्रणाली का प्रयोग किया जाएगा ।

(11) कंप्यूटर प्रणाली या पी के आई सर्वर जो अंकीय चिह्नक प्रमाणपत्र कृत्य करते हैं, उन कृत्यों को समर्पित होगे और उनका उपयोग किसी अन्य प्रयोजन के लिए नहीं किया जाएगा ।

(12) प्रणाली साफ्टवेयर का अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शन की पैरा 15 के अनुसार अक्षतता के लिए सत्यापन किया जाएगा ।

4. मीडिया भंडारण

प्रमाणन प्राधिकारी को सुनिश्चित करना चाहिए कि उसकी प्रणाली द्वारा प्रयुक्त भंडारण मीडिया पर्यावरण प्रकोप से जैसे तापमान, आर्द्रता और चुबकीय से संरक्षित हैं और उनका अनुसूची-2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शन सिद्धांतों की पैरा 8.3 और 8.4 के अनुसार परिवहन किया जाता है तथा प्रबंध किया जाता है ।

5. अपशिष्ट व्ययन

अंकीय चिह्नक प्रमाणपत्र के जनन, जारी करने, उत्पादन, और प्रबंधन से सहबद्ध सभी कृत्यों से संबंधित सूचना को भंडारण के लिए प्रयुक्त सभी मीडिया की नष्ट किए जाने या व्ययन के छोड़े जाने से पूर्व संवीक्षा की जाएगी ।

6. स्थलबाह्य प्रयुक्ति बैकअप

प्रमाणन प्राधिकारी को सुनिश्चित करना चाहिए कि स्थल बाह्य बैक अप, यदि कोई हो, के लिए सुविधाएं देश के भीतर होंगी और उनकी सुरक्षा का वही स्तर होगा जो प्रारंभिक प्रमाणन प्राधिकारी स्थल का होता है ।

7. परिवर्तन और आकृति प्रबंधन

1. प्रमाणन प्राधिकारी अवसंरचना के घटक (जैसे बीज लेखन अल्गोरिद्धम और इसके कुंजी प्राचल, प्रचालन प्रणाली, प्रणाली साफ्टवेयर, कंप्यूटर प्रणाली, पी के आई सर्वर, फायरवाल वस्तुगत सुरक्षा, प्रणाली सुरक्षा, प्रचालन प्रणाली आदि) का प्रत्येक वर्ष नई प्रौद्योगिक जोखिम के लिए पुनर्विलोकन किया जाएगा और पहचान किए गए जोखिमों के प्रबंधन के लिए घटकों की समुचित कार्रवाई योजना विकसित की जाएगी ।

2. ऐसे उयोजन साफ्टवेयर, प्रणाली साफ्टवेयर और हार्डवेयर जो शंकास्पद स्रोतों से उपाप्त किए जाते हैं, स्थापित किए जाएंगे और उनका उपयोग अंकीय चिह्नक प्रमाणपत्र के उत्पादन और प्रबंधन से सहबद्ध किसी कार्य के लिए नहीं किया जाएगा ।

3. साफ्टवेयर अपडेट्स और पैचेज का प्रमाणकर्ता प्राधिकारी प्रणाली पर कार्यान्वित किए जाने से पूर्व सुरक्षा प्रमाण के लिए पुनर्विलोकन किया जाएगा ।

4. प्रमाणकर्ता प्राधिकारी के लिए प्रयुक्त क्रांतिक प्रणाली में सुरक्षा भेद्यता को सुधारने के लिए साफ्टवेयर अपडेट्स और पैचेज का तत्परता से पुनर्विलोकन किया जाएगा और कार्यान्वित किया जाएगा ।

5. साफ्टवेयर अपडेट्स और पैचेज पर सूचना और प्रमाणकर्ता प्राधिकारी प्रणाली पर कार्यान्वयन को स्पष्ट रूप से तथा उचित रूप से प्रलेखीकृत किया जाएगा ।

8. नेटवर्क और संसूचना सुरक्षा

(1) प्रमाणन प्राधिकारी प्रणाली को सूचना अनुसूची 2 में किए गए प्रौद्योगिक सुरक्षा मार्गदर्शक सिद्धांतों की पैरा 17, पैरा 18, पैरा 19, और पैरा 20 के अनुसार अन्य प्रणालियों से क्रांतिक प्रणालियों और सेवाओं तक नेटवर्क पहुंच नियन्त्रण सुनिश्चित करने के लिए संरक्षित किया जाएगा ।

(2) प्रमाणन प्राधिकारी प्रणाली से बाह्य नेटवर्कों तक नेटवर्क संसंग (कनेक्शन) केवल उन संसंगों (कनेक्शनों) तक निर्बंधित होगा जो प्रमाणन प्राधिकारी के कृत्यकारी प्रक्रियाओं और सेवाओं को सुकर बनाने के लिए अत्यावश्यक है। बाह्य नेटवर्क से ऐसे नेटवर्क संसंग उचित रूप से सुरक्षित होंगे और नियमित रूप से मानीटर किए जाएंगे ।

(3) नेटवर्क संसंग (कनेक्शन) अंकीय चिह्नक प्रमाणपत्र के उत्पादन और प्रबंधन के कृत्य करनेवाली प्रणालियों से उन प्रणालियों को जोड़ने के लिए प्रारंभ किया जाना चाहिए जो रजिस्ट्रीकरण और निधान कृत्य कर रही है किंतु विपर्येण नहीं । यदि यह संभव नहीं है तो समकारी नियन्त्रण (जैसे परोक्षी का प्रयोग) को उन प्रणालियों को जो अंकीय चिह्नक प्रमाणन के उत्पादन और प्रबंधन के कृत्य कर रही हैं, संभावी आक्रमण से संरक्षित करने के लिए कार्यान्वित किया जाना चाहिए ।

(4) उन प्रणालियों को जो अंकीय चिन्हक प्रमाणन कृत्य कर रही है, अलग किया जाना चाहिए जिससे कि प्रमाणन कृत्य की गोपनीयता, अक्षतता और उपलब्धता के संकट के प्रयास के उनेक विगोपन को न्यूनतम किया जा सके ।

(5) नेटवर्क पर जुड़ी हुई प्रमाणन प्राधिकारी प्रणालियों के बीच संपर्क गोपनीयता और अक्षतता सुनिश्चित करने के लिए सुरक्षित होने चाहिए । उदाहरणार्थ, नेटवर्क पर जुड़ी हुई प्रमाणन प्राधिकारी प्रणालियों के बीच संपर्क असमिति किया जाए और अंकीय रूप से चिन्हन किया जाए ।

(6) अधिक्रमण खोजी उपकरण क्रांतिक नेटवर्क और पेरिमीटर नेटवर्कों को मानीटर करने तथा नेटवर्क के तथा सामरिक रीति में प्रवेश के प्रयास के प्रति प्रशासकों को सचेत करने के लिए लगाए जाने चाहिए ।

9..प्रणाली सुरक्षा लेखा परीक्षा प्रक्रिया

9.1. अभिलिखित घटना का प्रकार

(1) प्रमाणकर्ता प्राधिकारी को अपनी प्रणाली की सुरक्षा से संबंधित सभी घटनाओं का अभिलेख रखना चाहिए । अभिलेख आडित लाग फाइल में रखा जाना चाहिए और उसमें निम्नलिखित घटनाएं आती हैं –

- (i) चालू करने और बंद करने की प्रणाली ;
- (ii) प्रमाणन प्राधिकारी का उपयोजन चालू करना और बंद करना ;
- (iii) पासवर्ड्स सूजित करने, हटाने या निर्धारित करने का प्रयास और पी के आई मास्टर आफिसर, पी के आई आफिसर, या पी के आई प्रशासक के प्रणाली विशेषाधिकारों को परिवर्तित करना ;
- (iv) प्रमाणन प्राधिकारी की कुंजियों के परिवर्तन या उसके कोई अन्य ब्योरे ;
- (v) अंकीय चिन्हक प्रमाणपत्र सृजन नीतियों में परिवर्तन जैसे विधिमान्यता अवधि ;
- (vi) लाग इन और लाग आफ प्रयास ;
- (vii) नेटवर्क पर प्रमाणन प्राधिकारी की प्रणाली तक पहुंचने के अप्राधिकृत प्रयास ;
- (viii) प्रणाली फाइलों तक पहुंचने के अप्राधिकृत प्रयास ;
- (ix) स्वयं की कुंजियों का उत्पादन ;
- (x) अंकीय चिन्हक प्रमाणपत्रों का सृजन और प्रतिसंहरण ;
- (xi) हस्ताक्षरकर्ताओं को हटाने समर्थ और असमर्थ को प्रारंभ करने के तथा उनकी कुंजियों को अद्यतन करने तथा वापस लेने के प्रयास
- (xii) अंकीय चिन्हक प्रमाणपत्र और सी प्रमाणपत्र प्रतिसंहरण सूची (सी आर एल) निर्देशिका पर असफल पढ़ो और लिखों प्रचालन ।

(2) मानीटर करना और आडिट लाग

(i) प्रमाणन प्राधिकारी को स्वचालित सुरक्षा प्रबंध और मानीटरिक उपकरणों को प्रयोग के बारे में विचार करना चाहिए जो किसी भी समय सुरक्षा स्थिति का समग्र उपलब्ध कराते हैं । निम्नलिखित उपयोजन संव्यवहारों का अभिलेख रखा जाना चाहिए :

- (क) रजिस्ट्रीकरण ;
- (ख) प्रमाणन ;
- (ग) प्रकाशन ;
- (घ) निलंबन ; और
- (ङ) प्रतिसंहरण ।

(ii) अभिलेखों और लाग फाइलों का निम्नलिखित क्रियाकलापों के लिए नियमितरूप से पुनर्विलोकन किया जाना चाहिए :

- (क) दुरुपयोग ;
- (ख) त्रुटि ;
- (ग) सुरक्षा उल्लंधन ;
- (घ) विशेषाधिकार प्राप्त कृत्य का निष्पादन ;
- (ङ) पहुंच नियन्त्रण सूचियों में परिवर्तन ;
- (च) प्रणाली समाकृति में परिवर्तन ।

(3) सभी लाग चाहे वे इलैक्ट्रॉनिक हों या हस्तचालित साधनों से अनुरक्षित हों, घटनाओं की तारीख और समय तथा उस हस्ताक्षरकर्ता / अधीनस्थ/इकाई की पहचान अंतर्विष्ट करेंगे जिससे घटना कारित हुई ।

(4) प्रमाणन प्राधिकारी के इलैक्ट्रॉनिक से या हस्तचालित रूप से सुरक्षा जानकारी को संगृहीत और समेकित करना चाहिए जो प्रमाणन प्राधिकारी प्रणाली से उत्पादित नहीं होते हैं ।

- (i) वस्तुगत पहुंच लाग ;
- (ii) प्रणाली समाकृति परिवर्तन और अनुरक्षण ;
- (iii) कार्मिक परिवर्तन ;
- (iv) फर्क और सकट रिपोर्ट ;
- (v) मीडिया के नष्ट होने का अभिलेख जिसमें कुंजी सामग्री क्रियाशील करने का डाटा या निजी अभिदाता सूचना अंतर्विष्ट हो ।

(5) निर्णय लेना सुकर बनाने के लिए प्रमाणकर्ता प्राधिकारी द्वारा उपलब्ध कराई गई सेवाओं से संबंधित सभी करार और पत्राचार को चाहे इलैक्ट्रॉनिक रूप से या हस्तचालित रूप से एक ही स्थान में संगृहीत और समेकित किया जाना चाहिए ।

9.2 आडिट लाग मानीटर करने की आवृत्ति

प्रमाणकर्ता प्राधिकारी को सुनिश्चित करना चाहिए कि उसके आडिट लाग का उसके कार्मिकों द्वारा प्रत्येक दो सप्ताह में कम से कम एक बार पुनर्विलोकन किया जाता है और सभी महत्वपूर्ण घटनाओं का ब्यौरा आडिट संक्षिप्ति संक्षेप में दिया जाता है । ऐसे पुनर्विलोकन में यह सत्यापन किया जाना चाहिए कि लाग से छेड़छाड़ नहीं की गई है और तब संक्षिप्ति रूप में लागों में किसी चौकसी या अनियमितताओं का और विस्तार से अन्वेषण करना चाहिए । इन पुनर्विलोकनों के अनुसरण में की गई कार्रवाइयों को प्रलेखीकृत किया जाना चाहिए ।

9.3. आडिट लाग के लिए प्रतिधारण अवधि

प्रमाणकर्ता प्राधिकारी को चाहिए कि वह अपनी आडिट रिपोर्ट स्थल पर कम से कम दो मास तक रखे और तत्पश्चात् उन्हें अनुसूची 2 में दिए गए सूचना प्रौद्योगिकी सुरक्षा मार्गदर्शन की पैरा 8 में विहित रीति में प्रतिधारित करे ।

9.4. आडिट लाग का संरक्षण

इलैक्ट्रॉनिक आडिट प्रणाली के अंतर्गत लाग फाइलो को अप्राधिकृत रूप से देखने, उपातरित करने और हटाने से संरक्षित करने के लिए क्रिया विधि होनी चाहिए ।

हस्तचालित आडिट सूचना को अप्राधिकृत रूप से देखने, उपातरित करने और नष्ट करने से संरक्षित किया जाना चाहिए ।

9.5. आडिट लाग बैकअप प्रक्रिया

आडिट लाग और आडिट संक्षिप्तियों को यदि वे हस्तचालित रूप में हैं बैकअप किया जाना चाहिए या उनकी प्रति तैयार कराई जानी चाहिए ।

9.6. भेद्यता निर्धारण

आडिट प्रक्रिया में घटनाएं प्रणाली भेद्यता को मानीटर करने के लिए अभिलिखित की जानी चाहिए । प्रमाणकर्ता प्राधिकारी को सुनिश्चित करना चाहिए कि भेद्यता निर्धारण इन घटनाओं की मानीटर की गई परीक्षा के अनुसरण में किया जाता है पुनर्विलोकन किया जाता है और यदि आवश्यक हो तो पुनरीक्षण किया जाता है ।

10. अभिलेख आगार

(1) प्रमाणकर्ता प्राधिकारी द्वारा भंडारित और उत्पादित अंकीय विवृतक प्रमाणपत्र उसकी समाप्ति की तरीख के पश्चात् कम से कम सात वर्ष तक सुरक्षित रखे जाने चाहिए । इस अपेक्षा के अंतर्गत प्राइवेट हस्ताक्षर कुंजियों का बैक अप नहीं आता है ।

(2) आडिट सूचना जिसका व्यौरा पैरा 9 में दिया गया है, हस्ताक्षरकर्ता की बाबत करार सत्यापन पहचान और प्राधिकरण सूचना को कम से कम सात वर्ष तक सुरक्षित रखा जाना चाहिए ।

(3) प्रमाणकर्ता प्राधिकारी स्थल सहित देश के भीतर सुरक्षित रखी गई या बैक अप की गई सभी सूचना की दूसरी प्रति को तीन अवस्थाओं पर भंडारित किया जाना चाहिए और उसे केवल भौतिक सुरक्षा से या भौतिक और बीजलेखन संरक्षण के संयोजन से संरक्षित किया जाना चाहिए । ऐसे किसी द्वितीयक स्थल में पर्यावरण संकट जैसे तापमान, आर्द्रता और चुम्बकत्व से पर्याप्त संरक्षण उपलब्ध होना चाहिए । द्वितीयक स्थल कुछ घंटों में पहुंचने योग्य होना चाहिए ।

(4) प्रमाणकर्ता प्राधिकारी के प्रचालन, हस्ताक्षरकर्ता के उपयोजन, सत्यापन, पहचान, अधिप्रमाणन और हस्ताक्षरकर्ता के करार से संबंधित सभी सूचना देश के भीतर भंडारित की जाएगी । इस सूचना को नियन्त्रक की अनुमति से ही और जहां समुचित रूप से सांविधानिक वारंट या ऐसा विधिक रूप से प्रवर्तनशील दस्तावेज प्रस्तुत किया जाता है देश के बाहर ले जाया जाएगा ।

(5) प्रमाणकर्ता प्राधिकारी को कम से कम प्रत्येक छह मास में बैक अप की अक्षतता का सत्यापन करना चाहिए ।

(6) आंकड़े सतता के लिए आवधिक रूप से सत्यापित किया गया स्थानेतर भंडारित जानकारी ।

11. संकट और विनाश प्रत्युद्धरण

11.1. प्रमाणकर्ता प्राधिकारी को कारबार निरंतरता प्रक्रिया स्थापित करनी चाहिए जिसमें भ्रष्टाचरण की दशा में या कंप्यूटरिंग या नेटवर्किंग संसाधनों, नामित वेबसाइट, निधान, साफ्टवेयर और/ या डाटा के खो जाने की दशा में की जाने वाली कार्रवाई की रूपरेखा हो । जहां कोई निधान प्रमाणकर्ता प्राधिकारी के नियंत्रण में नहीं है वहां प्रमाणकर्ता प्राधिकारी को सुनिश्चित करना चाहिए कि निधान से साथ किसी करार में कारबार निरंतरता प्रक्रिया का उपबंध है ।

11.2. प्राकृतिक या अन्य प्रकार के विनाश के पश्चात् सुरक्षा सुविधा

प्रमाणकर्ता प्राधिकारी को विनाश पत्युद्धरण योजना स्थापित करनी चाहिए जिसमें प्राकृतिक या अन्य प्रकार के विनाश की दशा में सुरक्षित सुविधा पुनः स्थापित करने के लिए की जाने वाली कार्यवाही की रूप रेखा दी गई हो । जहां निधान प्रमाणकर्ता प्राधिकारी के नियंत्रण के अधीन नहीं है, वहां प्रमाणकर्ता प्राधिकारी को यह सुनिश्चित करना

चाहिए कि निधान के साथ किसी भी करार में यह उपबंध हो कि विनाश प्रत्युद्धरण योजना निधान द्वारा स्थापित की जाएगी तथा प्रलेखीकृत की जाएगी ।

11.3. आनुषंगिक प्रबंध योजना

प्रबंध द्वारा एकआकस्मिक प्रबंध योजना विकसित और अनुमोदित की जाएगी । योजना में निम्नलिखित क्षेत्र सम्मिलित होंगे :—

- (i) प्रमाणकर्ता प्राधिकारी प्रमाणन कुंजी संकट ;
- (ii) प्रणाली और नेटवर्क का किराए पर लेना ;
- (iii) वस्तुगत सुरक्षा का भंग ;
- (iv) अवसंरचना उपलब्धता ; और
- (v) कपटपूर्ण रजिस्ट्रीकरण और अंकीय चिह्नक प्रमाणपत्रों ;
- (vi) अंकीय चिह्नक प्रमाणपत्र निलंबन और प्रतिसंहरण सूचना ।

एक आनुषंगिक प्रतिक्रिया कार्य योजना प्रमाणकर्ता प्राधिकारी की आकस्मिकताओं के प्रति प्रतिक्रिया के प्रति तेयारी सुनिश्चित करने के लिए स्थापित की जाएगी । इस योजना में निम्नलिखित होंगे :

- (i) संकट नियंत्रण
- (ii) उपयोक्ता समुदाय को अधिसूचना (यदि लागू हो);
- (iii) प्रभावित अंकीय चिह्नक प्रमाणपत्र का प्रतिसंहरण (यदि लागू हो);
- (iv) कार्मिक व्यवहार घटनाओं का उत्तरदायित्व ;
- (v) सेवा व्यवधान प्रक्रिया का अन्वेषण ;
- (vi) सेवा पुनःस्थापन प्रक्रिया ;
- (vii) मानीटर करने और आडिट खोज विश्लेषण ; और
- (viii) मीडिया और लोक संबंध ।

12. कार्य के अनुसार अपेक्षित व्यक्तियों की संख्या

प्रमाणकर्ता प्राधिकारी को सुनिश्चित करना चाहिए कि कोई अकेला व्यक्ति अंकीय चिह्नक प्रमाणपत्र वितरक (सर्वर) और कम्प्यूटर वितरक (सर्वर) तक न पहुंचे जो प्रमाणकर्ता प्राधिकारी के अंकीय चिह्नक प्रमाणपत्र और प्राइवेट कुंजियों के उत्पादन जारी करने और प्रबंध से सहबद्ध सभी सूचना बनाए रखता है । कम से कम दो व्यक्तियों को जो अधिमानतः विभाजित तकनीक का जैसे दुहरे पासवर्ड उपयोग करते हैं अंकीय चिह्नक प्रमाणपत्र उत्पादन जारी करने और प्रमाणकर्ता प्राधिकारी के प्राइवेट कुंजी के उपयोजन और प्रबंध से सहबद्ध किसी क्रिया का समापन करना चाहिए ।

13. प्रत्येक भूमिका के लिए पहचान और अधिप्रमाणन

सभी प्रमाणकर्ता प्राधिकारी कार्मिकों को इसके पूर्व कि उन्हें :—

- (i) प्रमाणकर्ता प्राधिकारी स्थल के लिए पहुंच सूची में सम्मिलित किए जाने हैं
- (ii) प्रमाणकर्ता प्राधिकारी प्रणाली तक वस्तुगत पहुंच के लिए पहुंच सूची में सम्मिलित किया जाता है
- (iii) उन्हें उनकी प्रमाणकर्ता प्राधिकारी भूमिका का निष्पादन करने के लिए प्रमाणपत्र दिया जाता है,

(iv) पी के आई प्रणाली पर लेखा दिया जाता है ।

उनकी पहचान और अधिप्रमाणन का सत्यापन कराया जाना चाहिए ।

इनमें से प्रत्येक प्रमाणपत्र और लेखा (केवल प्रमाणकर्ता प्राधिकारी के हस्ताक्षर वाले प्रमाणपत्रों के सिवाय) —

(i) प्रत्यक्ष रूप से किसी व्यक्ति को मिले हुए माने जाने चाहिए

(ii) अंशधारिता नहीं होनी चाहिए

(iii) उस भूमिका के लिए प्राधिकृत कार्य तक निर्वधित किया जाना चाहिए, और

(iv) प्रक्रियात्मक नियंत्रण होना चाहिए ।

प्रमाणकर्ता प्राधिकारी के प्रचालन को अधिप्रमाणन और सममितता की तकनीक का उपयोग करके सुरक्षित किया जाना चाहिए जब वह अंशधारित नेटवर्क से पहुंच का है ।

14. कार्मिक सुरक्षा नियंत्रण

प्रमाणकर्ता प्राधिकारी को यह सुनिश्चित करना चाहिए कि इसके प्रचालन की बाबत कर्तव्य निभाने वाले सभी कार्मिकों की —

(i) लिखित रूप में नियुक्ति की गई हो ;

(ii) उन्हें उस पद के जो उन्हें भरना है, निबंधनों और शर्तों से संविदा या कानून द्वारा आबद्ध किया गया है ;

(iii) उन्हें उन कर्तव्यों की बाबत जो उन्हें निष्पादित करना है व्यापक प्रशिक्षण प्राप्त हुआ है ;

(iv) वे संवेदनशील प्रमाणकर्ता प्राधिकारी सुरक्षा संबंधी सूचना या हस्ताक्षरकर्ता की सूचना को प्रकट न करने के लिए कानून या संविदा द्वारा आबद्ध हो ;

(v) उन्हें ऐसा कर्तव्य न सौंपा गया हो जो प्रमाणकर्ता प्राधिकारी के कर्तव्यों के साथ उनके हित में विरोध पैदा करे ; और

(vi) प्रमाणकर्ता प्राधिकारी के प्रचालन क्रियान्वयन के लिए विरचित सूचना प्रौद्योकिगी सुरक्षा नीति और सुरक्षा मार्गदर्शन के सुसंगत पहुंच में से अवगत हो तथा उनमें प्रशिक्षित हो ।

15. प्रशिक्षण अपेक्षाएं

प्रमाणकर्ता प्राधिकारी को यह सुनिश्चित करना चाहिए कि वे सभी कार्मिक जो उसके प्रचालन की बाबत कर्तव्यों का निर्वहन कर रहे हैं निम्नलिखित में व्यापक प्रशिक्षण अवश्य प्राप्त करें—

(i) सूचना प्रौद्योगिक सुरक्षा नीति और प्रमाणकर्ता अधिकारी द्वारा बनाए गए मार्ग दर्शन के सिद्धान्तों के सुसंगत पहलू ;

(ii) प्रमाणकर्ता अधिकारी के तंत्र में प्रयोग किए जा रहे सभी पी के आई साप्टवेयर भाग ;

(iii) सभी पी के आई कर्ता हैं जिनका पालन करना उनके लिए अपेक्षित है ; और

(iv) विनाश प्रत्युद्धरण और कारबार निरंतरता प्रक्रिया ।

16. पुनःप्रशिक्षण आवृत्ति और अपेक्षा

पैरा 14 की अपेक्षाओं को प्रमाणकर्ता प्राधिकारी प्रणाली में परिवर्तनों को समाविष्ट करने के लिए व्यवहृत रखा जाना चाहिए और प्रमाणकर्ता प्राधिकारी को इन अपेक्षाओं का वर्ष में कम से कम एक बार पुनर्विलोकन करना चाहिए ।

17. कार्मिकों को प्रदाय किए गए प्रलेखन

प्रमाणकर्ता प्राधिकारी को चाहिए कि वह अपने कार्मिकों को अंकीय विह्नक प्रमाणपत्र पालिसियां जिसका यह समर्थन करता है, इसके प्रमाणन प्रक्रिया विवरण सूचना प्रोटोग्राफी सुरक्षा नीति और कोई विनिर्दिष्ट कानून नीतियां या संविदा जो उनके पद सुसगत हैं, उन्हें उपलब्ध कराए ।

18. कुंजी प्रबंध

18.1. उत्पादन

1. हस्ताक्षरकर्ता का कुंजी युग्म हस्ताक्षरकर्ता द्वारा उत्पादित किया जाएगा या हस्ताक्षरकर्ता की उपस्थिति में कुंजी उत्पादन प्रणाली पर उत्पादित किया जाएगा ।

2. कुंजी उत्पादन प्रक्रिया सांख्यिकी रूप से यादृच्छिक कुंजी मूल्य से जो ज्ञात आक्रमणों से प्रतिरक्षित है उत्पादित करेगा ।

18.2. कुंजियों का वितरण

कुंजी को एक सुरक्षित क्रियाविधि का प्रयोग करके जो गोपनीयता और अक्षतता सुनिश्चित करती हो, कुंजी उत्पादन प्रणाली द्वारा भंडारण युक्ति में (यदि कुंजी को कुंजी उत्पादन प्रणाली पर भंडारित किया जाता है) अंतरित किया जाएगा ।

18.3. भंडारण

(1) प्रमाणकर्ता प्राधिकारी कुंजियों छेड़छाड़ प्रतिरोधक युक्तियों में भंडारित की जाएंगी और पक्षकारों द्वारा जो प्रमाणकर्ता प्राधिकारी प्रणाली और प्रचालन के गठन और अनुरक्षण में अंतर्वलित नहीं हैं। केवल विभाजन नियंत्रण के अधीन क्रियाशील की जाएंगी प्रमाणकर्ता प्राधिकारी कुंजी को छेड़छाड़ प्रतिरोधक असमित माध्यम में या भंडारित की जाएंगी या कुंजी परिस्कर के अधीन में विभाजित की जाएंगी ।

(2) प्रमाणकर्ता प्राधिकारी कुंजी परिस्कर या सुनिश्चित करेगा कि प्रमाणकर्ता प्राधिकारी कुंजी घटक या क्रियाशील करने का कोड सर्वदा अनन्य अभिरक्षा के अधीन रहता है। कुंजी परिस्कर का परिवर्तन प्रमाणकर्ता प्राधिकारी प्रबंध और द्वारा अनुमोदित और प्रलेखित किया जाएगा ।

18.4. प्रचलन

(1) प्रणाली और साप्टवेयर अक्षतता जांच प्रमाणकर्ता प्राधिकारी कुंजी भरण के पहले की जानी चाहिए ।

(2) प्रमाणकर्ता प्राधिकारी कुंजी की अभिरक्षा और उस तक पहुंच विभाजन नियंत्रण के अधीन होगी। विशिष्ट रूप से प्रमाणकर्ता प्राधिकारी कुंजी भरण विभाजन नियंत्रण के अधीन किया जाएगा ।

18.5. उपयोगताओं को प्रमाणकर्ता प्राधिकारी लोक कुंजी परिदान

प्रमाणकर्ता प्राधिकारी की लोक सत्यापन कुंजी अंकीय विह्नक प्रमाणपत्र धारक को प्रमाणपत्र प्रबंध प्रोटोकालके पी.के. आई.एक्स-3 के अनुसार लाइन पर संव्यवहार में या किसी समतुल्य सुरक्षित रीति के माध्यम से परिदृत की जाएगी ।

19. प्राइवेट कुंजी संरक्षण और बैक अप

(1) प्रमाणकर्ता प्राधिकारी और हस्ताक्षरकर्ता धारक को प्राइवेट कुंजियों के प्रकटन से संरक्षित रखना चाहिए ।

(2) प्रमाणकर्ता प्राधिकारी प्राइवेट कुंजियों को बैक अप कर सकता है। बैक अप कुंजियों को एन्क्रीप्टेड रूप में भंडारित किया जाना चाहिए और उस स्तर पर संरक्षित किया जाना चाहिए जो कुंजी के प्रारंभिक कथन के भंडारण के लिए अपनाई जाने वाले स्तर से नीचे की न हो ।

(3) प्रमाणकर्ता प्राधिकारी प्राइवेट कुंजी बैंक अप उस स्थान से जहां मूल कुंजी भंडारित की गई है, दूर सुरक्षित भंडारित सुविधा में भंडारित की जानी चाहिए ।

20. प्राइवेट कुंजी को नष्ट करने की पद्धति

प्राइवेट कुंजी के प्रयोग की समाप्ति पर कंप्यूटर की स्मृति (मेमोरी) में की सभी प्रतियां और अंशधारित डिस्क स्थान (स्पेस) को उपरिलेखन कर सुरक्षित रूप से नष्ट किया जाना चाहिए । प्राइवेट कुंजी नष्ट करने की प्रक्रिया का प्रमाणन प्रक्रिया निवारण या सार्वजनिक रूप से उपलब्ध अन्य दस्तावेज में वर्णन किया जाना चाहिए ।

21. लोक और प्राइवेट कुंजियों के लिए प्रचलन अवधि

21.1. कुंजी परिवर्तन

- (1) प्रमाणकर्ता प्राधिकारी तथा हस्ताक्षरकर्ता कुंजियों का नियतकालिक रूप परिवर्तित किया जाएगा ।
- (2) कुंजी परिवर्तन पर कुंजी उत्पादन मार्गदर्शक सिद्धान्त के अनुसार कार्यवाही की जाएगी ।
- (3) प्रमाणकर्ता प्राधिकारी हस्ताक्षरकर्ता का आश्रय लेने वाले पक्षकारों को अंकीय चिह्नक प्रमाणपत्र पर हस्ताक्षर करने के लिए प्रमाणकर्ता प्राधिकारी द्वारा प्रयुक्त नए कुंजी युग्म में किसी परिवर्तन के बारे में युक्तियुक्त सूचना उपलब्ध कराएगा ।
- (4) प्रमाणकर्ता प्राधिकारी परिभाषित करेगा कि उसकी कुंजी प्रक्रिया जो प्रक्रिया की विश्वासनीयता यह दर्शित करके सुनिश्चित करता है कि कुंजी के परस्पर युग्म जाने का जैसे नई कुंजी का पुरानी कुंजी के साथ घालमेल (टुकड़े) करके हस्ताक्षर करने का उत्पादन करना होता है ।

सभी कुंजियों की विधि मान्यता अवधि पांच वर्ष से अधिक नहीं होनी चाहिए ।

सुझाई गई विधिमान्य अवधियां :

- (क) प्रमाणकर्ता प्राधिकारी की मूल कुंजियां और सहबद्ध प्रमाणपत्र पांच वर्ष ;
- (ख) प्रमाणकर्ता प्राधिकारी प्राइवेट हस्ताक्षर करने की कुंजी — दो वर्ष ;
- (ग) हस्ताक्षरकर्ता के लोक — इनक्रीष्ण और अंकीय चिह्नक प्रमाणपत्र कुंजी — तीन वर्ष ;
- (घ) हस्ताक्षरकर्ता की प्राइवेट इनक्रीष्ण कुंजी — तीन वर्ष ।

विशिष्ट कुंजी समयावधि का उपयोग विभागीय आशंका जोखिम निर्धारण के अनुसार अवधारित किया जाना चाहिए

21.2. नष्ट किया जाना

प्रमाणकर्ता प्राधिकारी के हस्ताक्षर प्राइवेट कुंजी के प्रयोग की समाप्ति पर प्राइवेट कुंजी के सभी घटकों तथा उसकी सभी बैंक अप प्रतियों को सुरक्षित रूप से नष्ट कर दिया जाएगा ।

21.3. कुंजी संकट

(1) ऐसे मामलों को सुलझाने के लिए एक प्रक्रिया पहले स्थापित की जाएगी जहां प्रमाणकर्ता प्राधिकारी अंकीय चिह्नक प्राइवेट कुंजी का संकट उद्भूत हुआ है । ऐसे मामले में प्रमाणकर्ता प्राधिकारी सभी प्रभावित हस्ताक्षरकर्ता अंकीय चिह्नक प्रमाणपत्रों को तत्काल प्रतिसंहृत करेगा ।

(2) प्रमाणकर्ता प्राधिकारी प्रमाणन प्राइवेट कुंजी संकट की दशा में प्रमाणकर्ता प्राधिकारी सभी प्रभावित हस्ताक्षरकर्ता अंकीय चिह्नक प्रमाणपत्रों को तत्काल प्रतिसंहृत कर सकेगा ।

(3) प्रमाणकर्ता प्राधिकारी लोक कुंजियों को आडिट और अन्वेषण अपेक्षाओं को सुकर बनाने के लिए स्थायी रूप से अभिलेखा भारित किया जाएगा ।

(4) प्रमाणकर्ता प्राधिकारी लोक कुंजियों के अभिलेखाकार को अप्राधिकृत उपांतरों से सुरक्षित किया जाएगा ।

22. हस्ताक्षरकर्ता की सूचना की गोपनीयता

(1) प्रमाणकर्ता प्राधिकारी की अभिलेखा के अधीन हस्ताक्षरकर्ता की एकांतता और गोपनीयता संरक्षित करने के लिए प्रक्रिया और सुरक्षा नियंत्रण कार्यान्वयिता किए जाएंगे । हस्ताक्षरकर्ता द्वारा उपलब्ध कराई गई गोपनीय सूचना को हस्ताक्षरकर्ता की सम्मति के सिवाय तृतीय पक्षकार को प्रकट नहीं किया जाना चाहिए जब तक कि सूचना का विधि के या किसी न्यायालय के आदेश के अधीन प्रकट किया जाना अपेक्षित नहीं है ।

(2) हस्ताक्षरकर्ताओं द्वारा अंकीय चिह्नक प्रमाणपत्र को प्रथा पर आंकड़ों का तथा प्रमाणकर्ता प्राधिकारी अपने प्रचालन के दौरान उत्पादित हस्ताक्षरकर्ता के क्रियाकलापों से संबंधित संव्यवहार विषयक आंकड़ों को हस्ताक्षरकर्ता की एकांतता को सुनिश्चित करने के लिए संरक्षित किया जाएगा ।

(3) प्रमाणकर्ता प्राधिकारी और उसके हस्ताक्षरकर्ता के बीच एक सुरक्षित माध्यम अंकीय चिह्नक प्रमाणपत्र जारी किए जाने की प्रक्रिया के दौरान विनियम की प्रामाणिकता, अक्षतता और गोपनीयता (अर्थात् अंकीय चिह्नक प्रमाणपत्र, पासवर्ड (संकेतशब्द), प्राइवेट कुंजी का पारेषण) सुनिश्चित करने के लिए स्थापित किया जाएगा ।

अनुसूची-4

अंकीय चिह्नहक प्रमाणपत्र जारी करने के लिए आवेदन का प्रपत्र [प्रियं २३ डिसेम्बर]

व्यष्टिक / अविभक्त हिंदू कुटुम्ब आवेदकों के लिए

1. पूरा नाम * अविभक्त हिंदू कुटुम्ब की दशा में कर्ता का नाम

अंतिम नाम और उप नाम _____

प्रथम नाम _____

मध्य नाम _____

2. क्या आप कभी किसी अन्य नाम से जाने जाते रहे हैं ? यदि हां, तो

अंतिम नाम/उपनाम _____

प्रथम नाम _____

मध्यम नाम _____

3. पता

निवास स्थान का पता- *

फ्लैट/डोर/ब्लाक सं०

परिसर/भवन/ग्राम का नाम

सड़क /स्ट्रीट/गली/डाकघर

क्षेत्र/अवस्थान/तालुका/उपखंड

नगर/शहर जिला

राज्य/संघ राज्य क्षेत्र

टेलीफोन सं०

पिन:

फैक्स

मोबाइल फोन नं०

कार्यालय का पता-

कार्यालय का नाम

फ्लैट/डोर/ब्लाक सं०

परिसर/भवन/ग्राम का नाम

सड़क/स्ट्रीट/गली/डाकघर _____
 क्षेत्र/अवस्थान/तालुका/उपखंड _____
 नगर/शहर जिला _____
 राज्य/संघ राज्य क्षेत्र _____ पिन _____
 टेलीफोन सं. _____
 फैक्स _____

4. पत्राचार के लिए पता:- * क या खं, जो लागू हो उस पर सही (✓) निशान लगाएं

5. पिता का नाम *

अंतिम नाम/उपनाम _____
 प्रथम नाम _____
 मध्य नाम _____

6. लिंग- * (केवल व्यष्टि आवेदक के लिए) जो लागू हो उस पर सही (✓) निशान लगाएं : पुरुष / स्त्री

7. जन्म की तारीख(दिन/मास/वर्ष) *

8. राष्ट्रीयता- *

9. विदेशी राष्ट्रिक की दशा में, वीजा के ब्यौरे

10. क्रेडिट कार्ड के ब्यौरे

क्रेडिट कार्ड का प्रकार

क्रेडिट कार्ड संख्यांक

जिसके द्वारा जारी किया गया

11. ई मेल का पता

12. वेब यू आर एल पता

13. पासपोर्ट के विवरण #

पासपोर्ट संख्या

पासपोर्ट जारी करने वाला प्राधिकारी

पासपोर्ट के अवसान की तारीख

14. मतदाता का पहचान पत्र संख्यांक #

15. आयकर स्थायी लेखा (पैन) संख्यांक #

16. आई एस पी का ब्यौरा*

आई एस पी का नाम

आई एस पी के वेबसाइट का पता, यदि कोई हो

आई एस पी में आपका उपयोक्ता नाम, यदि कोई हो

17. वैयक्तिक वेब पेज यू आर एल, यदि कोई हो

कंपनी/फर्म व्यष्टिकों के निकाय/व्यक्तियों के संगम/स्थानीय प्राधिकारी के लिए

18. रजिस्ट्रीकरण संख्यांक

19. निगमन/करार/भागीदारी अथवा न्यास बिलेख विरचना की तारीख*

20. कारबार की विशिष्टियां, यदि कोई हो

प्रधान कार्यालय

कार्यालय का नाम

फ्लैट/डोर/ब्लाक संख्या _____
 परिसर/भवन /ग्राम का नाम _____
 सड़क/स्ट्रीट/गली/डाकघर _____
 क्षेत्र/अवस्थसान/तालूका/उपप्रखंड _____
 नगर/शहर/ज़िला _____
 राज्य/संघ राज्य क्षेत्र _____
 टेलीफोन नं० _____
 फैक्स _____
 वेब पेज यू आर एल, यदि कोई हो _____
 शाखाओं की संख्या _____
 कारबार की प्रकृति _____
 21. आयकर स्थायी लेखा (पैन) संख्यांक* _____
 22. पिछले वित्तीय वर्ष में आवर्त (टर्न ओवर) _____

23. भागीदारों/सदस्यों/निदेशकों के नाम, पते आदि (अधिक व्यक्तयों की दशा में सूचना के लिए निम्नलिखित प्ररूप में अतिरिक्त शीटें जोड़ें)
 भागीदारों / सदस्यों / निदेशकों के ब्यौरे
 भागीदारों/सदस्यों/निदेशकों
 के की संख्या _____
 पूरा नाम _____
 अंतिम नाम/उपनाम _____
 प्रथम नाम _____
 मध्यम नाम _____

पता

फ्लैट/डोर/ब्लाक सं० _____
 परिसर/भवन/ग्राम का नाम _____
 सड़क/स्ट्रीट/गली/डाकघर _____
 क्षेत्र/अवस्थसान/तालूका/उपप्रखंड _____
 नगर/शहर/ज़िला _____
 राज्य/संघराज्य क्षेत्र _____
 टेलीफोन सं० _____
 फैक्स सं० _____
 मोबाइल फोन सं० _____

राष्ट्रीयता

विदेशी राष्ट्रिक की दशा में, वीजा के ब्यौरे _____

पासपोर्ट ब्यौरा #

पासपोर्ट सं० _____
 पासपोर्ट जारी करने वाला प्राधिकारी _____
 पासपोर्ट के अवसान की तारीख _____
 मतदाता का परिचय पत्र सं० # _____
 आयकर स्थायी लेखा (पैन) सं० _____
 ई-मेल पता _____
 वैयक्तिक वेब पेज यू आर एल, यदि कोई है _____

सरकारी संगठनों/अभिकरणों के लिए *

24. संगठन/अभिकरण की विशिष्टियां

संगठन का नाम	_____
प्रशासकीय मंत्रालय/विभाग	_____
राज्य/केन्द्रीय सरकार के अधीन	_____
फ्लैट/डोर/ब्लॉक सं०	_____
परिसर/भवन/ग्राम का नाम	_____
सड़क/स्ट्रीट/गली/डाकघर	_____
क्षेत्र/अवस्थसान/तालुका/उपखंड	_____
नगर/शहर/जिला	_____
राज्य/संघराज्य क्षेत्र	_____
टेलीफोन सं०	_____
फैक्स सं०	_____
संगठन के अध्यक्ष का नाम	_____
पदनाम	_____
ई-मेल का पता	_____

25. बैंक के ब्यौरे

बैंक का नाम *

शाखा *

बैंक खाता संख्या *

बैंक खाते का प्रकार *

26. अपेक्षित अंकीय चिह्नक प्रमाण पत्र का प्रकार*

तारीख

आवेदक के हस्ताक्षर

अनुदेश: 1. * से चिह्नांकित स्तंभ अनिवार्य रूप से लागू हैं।

2. # से चिह्नांकित स्तंभों के लिए कम-से-कम एक स्तंभ का ब्यौरा देना अनिवार्य है।

3. स्तंभ संख्या 1 से 17 व्यष्टिक आवेदकों द्वारा भरे जाने हैं।

4. स्तंभ संख्या 18 से 23 तब भरे जाने हैं यदि आवेदक कंपनी/फर्म व्यष्टिकों का निकाय/व्यक्तियों का संगम/स्थानीय प्राधिकारी/न्यास हैं।

5. स्तंभ 24 तब भरा जाना है यदि आवेदक सरकारी संगठन है।

6. स्तंभ संख्या 25 और 26 सभी आवेदकों द्वारा भरा जाना है।

अनुसूची 5

शब्दावली

स्वीकार करना (अंकीय चिह्नक प्रमाणपत्र)

किसी अंकीय चिह्नक प्रमाणपत्र आवेदक द्वारा, इसकी सूचनात्मक अंतर्वस्तुओं को जानते हुए या उनकी सूचना लेने पर, किसी अंकीय चिह्नक प्रमाणपत्र के अनुमोदन का प्रदर्शन करना ।

अभिगम

किसी कंप्यूटर, कंप्यूटर तंत्र या कंप्यूटर नेटवर्क में प्रवेश करना, तर्कसंगत, गणितीय या स्मृति, फलन साधनों को अनुदेश देना या उन्हें संसूचित करना ।

अभिगम नियंत्रण

केवल उपयोक्ताओं, क्रमादेशों या अन्य कंप्यूटर तंत्रों को प्रधिकृत करने के लिए किसी कंप्यूटर के साधनों तक अभिगम को सीमित करने की प्रक्रिया ।

प्रत्यायन

नियंत्रक द्वारा एक औपचारिक यह घोषणा कि कोई विशिष्ट सूचना तंत्र, वृत्तिक या अन्य क्रमचारी या संविदाकार या संगठन कतिपय कर्तव्यों के पालन के लिए और रक्षोपायों के विहित समुच्चय का प्रयोग करते हुए विनिर्दिष्ट सुरक्षा मोड में प्रचालन करने के लिए अनुमोदित है ।

प्राधिकार प्रतिसंहृत सूची (प्रा.प्र.सू.)

प्रतिसंहृत प्रमाणन प्राधिकारी प्रमाणपत्रों की सूची । प्रा.प्र.क्रास प्रमाणपत्रों के लिए प्रा.प्र.सू., प्र.प्र.सू. है ।

प्राप्तकर्ता

ऐसा व्यक्ति जो प्रवर्तक द्वारा इलेक्ट्रॉनिक अभिलेख प्राप्त करने के लिए आशयित है किंतु इसमें कोई मध्यवर्ती सम्मिलित नहीं है ।

सहबद्ध प्रमाणपत्र

किसी सहबद्ध व्यक्ति को जारी किया गया प्रमाणपत्र । (सहबद्ध व्यक्तिक भी देखिए)

अभिपुष्ट करना / अभिपुष्टि

यह कथन करना या आचरण द्वारा यह उपर्युक्त करना कि डाटा सही है या सूचना सत्य है ।

अंकीय चिह्नक लगाना

उसके व्याकरणीय रूप भेदों और सजातीय पदों सहित अंकीय चिह्नक लगाने से किसी व्यक्ति द्वारा किसी इलेक्ट्रॉनिक अभिलेख को अंकीय चिह्नक द्वारा अधिप्रमाणित करने के प्रयोजन के लिए अपनाई गई कोई रीति या प्रक्रिया अभिप्रेत है ।

उर्फ

कोई छव्मनाम ।

आवेदक (प्रा.प्रा. आवेदक ; प्रमाणपत्र आवेदक देखिए)

उपयोजन साफ्टवेयर

ऐसी कोई प्रक्रिया जो किसी उपयोजन समस्या के समाधान के लिए विनिर्दिष्ट है । यह उपयोग करके अंतिम उपयोक्ता द्वारा या उसके लिए कोड की गई ऐसी साफ्टवेयर है जो कोई सेवा प्रदान करती है या उपयोक्ता के कार्य से संबंधित है ।

उपयोजन तंत्र

उत्पादों का ऐसा समूह, जिन्हें वाणिज्यिक डाटा प्रसंस्करण, कार्यालय और संचार परिस्थितियों का समाधान करने के लिए और साथ ही सभी आकार के कारबारों के लिए साधारण, संगत क्रमादेशक और उपयोग करके अंतिम उपयोक्ता अंतरापृष्ठ उपलब्ध कराने के लिए डिजाइन किया गया है।

पुरामंडार

सुरक्षा, पूर्तिकर या लेखा परीक्षा प्रयोजनों के लिए, किसी दी गई समयावधि के लिए अभिलेखों और सहयुक्त जर्नलों के भंडारण के लिए।

आश्वासन

किसी विनिर्दिष्ट सेवा को उपलब्ध कराने और बनाए रखने के लिए सद्भाविक प्रयासों से समर्थित ऐसे कथन या आचरण जो कोई साधारण आशय प्रस्तुत करने के लिए आशयित है। “आश्वासन” से आवश्यक रूप से इस बात की प्रत्याभूति विवक्षित नहीं होती है कि सेवा पूर्णतया और समाधानप्रद रूप में की जाएगी। आश्वासन, जब तब कि अन्यथा स्पष्ट रूप से उपदर्शित न हो बीमा, वचन, प्रत्याभूति और वारंटी से भिन्न हैं।

असमति गूढ़ तंत्र

सुरक्षित कुंजी युग्म का एक तंत्र जिसमें अंकीय चिह्नक सृष्टि करने के लिए प्राइवेट कुंजी और अंकीय चिह्नक के सत्यापन के लिए लोक कुंजी है।

लेखा परीक्षा

यह विधिमान्य करने की प्रक्रिया कि नियंत्रक अपने स्थान पर है और अपने प्रयोजनों के लिए पर्याप्त है। इसमें किसी सूचना तंत्र में घुसपैठ या दुरुपयोग का पता लगाने के लिए रिकार्डिंग और विश्लेषणात्मक क्रियाकलाप सम्मिलित हैं। किसी लेखा परीक्षा द्वारा भिली अपर्याप्तताएं, समुचित प्रबंधन कार्मिक को रिपोर्ट की जाएंगी।

लेखा परीक्षा संस्करण पर्य

तंत्र क्रियाकलापों का, प्रसंस्करण का दस्तावेजी साक्ष्य उपलब्ध कराने वाला ऐसा कालानुक्रम अभिलेख जो प्रबंधन कर्मचारिवृन्द को किसी संव्यवहार के दौरान, उसके प्रारंभ से अंतिम परिणाम के निर्गम तक प्रत्येक घटना के प्रतिवर्ती या उस तक ले जाने वाले कथनों और क्रियाकलापों के क्रम के पुनर्निर्माण, पुनर्विलोकन और परीक्षा करने में समर्थ बनाता है।

अधिप्रमाणित अभिलेख

अधिप्रमाणन के समुचित आश्वासनों या निर्भर करने वाले पक्षकार द्वारा सत्यापित अंकीय चिह्नक सहित किसी संदेश के साथ हस्ताक्षरित दस्तावेज, तथापि, निलंबन और प्रतिसंहरण अधिसूचना प्रयोजनों के लिए, ऐसे अधिसूचना संदेश में अंतर्विष्ट अंकीय चिह्नक, अंकीय चिह्नक प्रमाणपत्र में अंतर्विष्ट लोक कुंजी से तत्संबंधी प्राइवेट कुंजी द्वारा सृष्टि किए जाने चाहिए।

अधिप्रमाणन

किसी व्यक्ति की पहचान की पुष्टि करने के लिए या किसी विनिर्दिष्ट सूचना की समग्रता साबित करने के लिए प्रयोग की गई प्रक्रिया। संदेश अधिप्रमाणन में, उसके स्रोत का अवधारण और यह सत्यापन कि इसे पारगमन में उपांतरित या प्रतिसंथापित नहीं किया गया है, अंतर्विलित है। [सत्यापन (अंकीय चिह्नक) भी देखिए।]

प्राधिकार

अधिकारों का, जिसमें विनिर्दिष्ट सूचना या साधन तक अभिगमन करने की सामर्थ्य सम्मिलित है, प्रदान किया जाना।

उपलब्धता

ऐसी सीमा, जहां तक सूचना या प्रक्रियाएं, किसी प्राधिकृत ईकाई द्वारा भाग किए जाने पर, साधनों तक प्राधिकृत अभिगम और काल-क्रांतिक प्रचालनों का समय से किया जाना अनुज्ञात करते हुए, युक्तियुक्ति रूप से उपलब्ध और उपयोज्य है।

पूर्तिकर

ऐसे समय पर, जब पूर्तिकर लिया गया था, आवश्यक प्रसंस्करण का वापिस प्रत्युद्धरण करने के प्रयोजन के लिए क्रांतिक सूचना, डाटा और साफ्टवेयर की प्रतिलिपि लेने की प्रक्रिया।

बंधन

किसी प्रमाणीकरण प्राधिकारी द्वारा किसी नामित सत्ता और उसकी लोक कुंजी के बीच संबंध की अभिपूष्टि।

प्रमाणपत्र

प्रमाणीकरण प्राधिकारी द्वारा जारी किया गया अंकीय चिह्नक प्रमाणपत्र।

प्रमाणपत्र शृंखला

प्रमाणपत्रों की कोई ऐसी क्रमित सूची जिसमें उपयोग करके समाप्त करने वाला उपयोक्ता ग्राहक प्रमाणपत्र और प्र.प्रा. प्रमाणपत्र अंतर्विष्ट है। (विधिमान्य प्रमाणपत्र देखिए)

प्रमाणपत्र अवसान

अंकीय चिह्नक प्रमाणपत्र में विनिर्दिष्ट ऐसा समय और तारीख जब किसी पूर्वतर निलंबन या प्रतिसहरण पर ध्यान दिए बिना, प्रचालन अवधि समाप्त होती है।

प्रमाणपत्र विस्तारण

किसी अंकीय चिह्नक प्रमाणपत्र का विस्तारण क्षेत्र, जो प्रमाणित, प्रमाणित अंशदाता, अंकीय चिह्नक प्रमाणपत्र जारीकर्ता और / या प्रमाणीकरण प्रक्रिया होने के कारण लोक कुंजी की बाबत अतिरिक्त सूचना दे सकेगा। मानक विस्तारण आई एस ओ / आई ई सी 9594-8 : 1995 (x. 509) के सशोधन 1 में परिमाणित है। कस्टम विस्तारण हित के समुदायों द्वारा भी परिमाणित किया जा सकता है।

प्रमाणपत्र जारी किया जाना

प्रमाणीकरण प्राधिकारी द्वारा अंकीय चिह्नक प्रमाणपत्र सृष्ट करने और अंकीय चिह्नक प्रमाणपत्र में सूचीबद्ध अंकीय चिह्नक प्रमाणपत्र आवेदक (जिसका अंशदाता बनना प्रत्याशित है) को इसकी अंतर्वस्तु की सूचना देने में की गई कार्यवाही।

प्रमाणपत्र प्रबंधन (अंकीय चिह्नक प्रमाणपत्र का प्रबंधन)

प्रमाणपत्र प्रबंधन में अंकीय चिह्नक प्रमाणपत्रों का भंडारण, वितरण, प्रसार, लेखा, प्रकाशन, समझौता वसूली, प्रतिसंहरण और प्रशासन सम्मिलित है, किंतु यह इन्हीं तक ही सीमित नहीं है। कोई प्रमाणीकरण प्राधिकारी, अंशदाता अंकीय चिह्नक प्रमाणपत्रों के लिए रजिस्ट्रीकरण प्राधिकारी के रूप में सेवा करके अंकीय चिह्नक प्रमाणपत्र प्रबंधन कृत्यों को करता है। प्रमाणीकरण प्राधिकारी, जारी और स्वीकृत किए गए अंकीय चिह्नक प्रमाणपत्रों को प्रकाशन द्वारा विधिमान्य के रूप में पदाभिहित करता है।

प्रमाणपत्र नीति

अंकीय चिह्नक प्रमाणपत्र प्रबंधन के दौरान किए गए इलैक्ट्रॉनिक संव्यवहारों के सामंजस्य में प्रशासनिक नीति का एक विशेष रूप। प्रमाणपत्र नीति, अंकीय प्रमाणपत्रों के जनन, उत्पादन, वितरण, लेखा, समझौता वसूली और प्रशासन से सहबद्ध सभी पहलुओं पर प्रकाश डालती है। अप्रत्यक्ष रूप से प्रमाणपत्र नीति, प्रमाणपत्र आधारित सुरक्षा तंत्र से सुरक्षित संचार तंत्र का प्रयोग करके लिए गए संव्यवहारों को भी शासित कर सकती है। क्रांतिक

प्रमाणपत्र विस्तारों के नियंत्रण द्वारा, ऐसी नीतियां और सहबद्ध प्रवर्तन प्रौद्योगिकी, विशिष्ट उपयोजनों द्वारा अपेक्षित सुरक्षा सेवाओं के उपबंधों का समर्थन कर सकती है।

प्रमाणपत्र प्रतिसंहरण (प्रमाणपत्र प्रतिसंहृत करें, देखिए)

प्रमाणपत्र प्रतिसंहरण सूची (प्र.प्र.सू.)

ऐसे पहचान किए गए अंकीय चिह्नक प्रमाणपत्रों के, जिन्हें उनके अवसान की तारीख से पूर्व निलंबित या प्रतिसंहृत किया गया है, प्रमाणीकरण प्राधिकारी द्वारा अंकीय रूप से हस्ताक्षरित आवधिक (या अत्यावश्यक) रूप से जारी की गई सूची। सूची साधारणतया प्र.प्र.सू. जारीकर्ता का नाम, जारी किए जाने की तारीख अगली प्र.प्र.सू. जारी किए जाने की नियत तारीख, निलंबित या प्रतिसंहृत अंकीय चिह्नक प्रमाणपत्रों के क्रम संख्यांक और निलंबन तथा प्रतिसंहरण का विनिरिदिष्ट समय और कारण उपदर्शित करती है।

प्रमाणपत्र क्रम संख्यांक

ऐसा मान जो किसी प्रमाणीकरण प्राधिकारी द्वारा सृष्ट किसी अंकीय चिह्नक प्रमाणपत्र की सुस्पष्ट रूप से पहचान करता है।

प्रमाणपत्र चिह्नांकन अनुरोध (प्र.चि.अ.)

किसी अंकीय चिह्नक प्रमाणपत्र आवेदन का मशीन पठन योग्य रूप।

प्रमाणपत्र निलंबन (प्रमाणपत्र निलंबित करें, देखिए)

प्रमाणीकरण / प्रमाणित करना

प्रमाणीकरण प्राधिकारी द्वारा अंकीय चिह्नक प्रमाणपत्र जारी किए जाने की प्रक्रिया।

प्रमाणीकरण प्राधिकारी (प्र.प्रा.)

ऐसा कोई व्यक्ति, जिसे सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 24 के अधीन अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए अनुज्ञाप्ति प्रदान की गई है।

प्रमाणन प्राधिकारी साफ्टवेयर

ईकाईयों की कुंजियों के प्रबंधन के लिए अपेक्षित गूदालेखी साफ्टवेयर।

प्रमाणन प्राधिकारी तंत्र

प्रमाणन प्राधिकारी द्वारा, अंकीय चिह्नक प्रमाणपत्र के जनन, उत्पादन, उसे जारी करने और उसका प्रबंधन करने के लिए प्रयोग में लाए गए सभी हार्डवेयर और साफ्टवेयर (उदाहरणार्थ कंप्यूटर, पी के आई सर्वर, चालक्रम युक्तियां आदि)

प्रमाणन प्रक्रिया विवरण (प्र.प्र.वि.)

प्रमाणन प्राधिकारी द्वारा ऐसी प्रक्रियाओं को विनिर्दिष्ट करने के लिए, जिन्हें प्रमाणन प्राधिकारी अंकीय चिह्नक प्रमाणपत्रों को जारी करने के लिए अपनाता है, जारी किया गया विवरण।

प्रमाणकर्ता (जारी करने वाला प्राधिकारी देखिए)

चुनौतीपूर्ण वाक्यांश

ऐसे अंकों और / या अक्षरों का समुच्चय, जिन्हें अंकीय चिह्नक प्रमाणकर्ता आवेदक द्वारा, प्रमाणन प्राधिकारी को, अंकीय चिह्नक प्रमाणपत्र आवेदन के साथ संसूचित करने के लिए चुना गया है और जिनका प्रमाणन प्राधिकारी द्वारा प्रमाणन प्रक्रिया विवरण की अपेक्षा अनुसार विभिन्न प्रयोजनों के लिए अंशदाता को अधिप्रमाणित करने के लिए प्रयोग किया गया है। चुनौतीपूर्ण वाक्यांश का उपयोग गुप्त शेयर धारक द्वारा किसी गुप्त शेयर जारीकर्ता को स्वयं को अधिप्रमाणित करने के लिए भी किया जाता है।

प्रमाणपत्र वर्ग

विनिर्दिष्ट स्तर की विश्वसनीयता का अंकीय चिट्ठक प्रमाणपत्र ।

ग्राहक उपयोजन

ऐसा उपयोजन जो व्यक्तिक कंप्यूटर या कार्यस्थान पर उपलब्ध रहता है और कोई प्रचालन करने के लिए सर्वर पर निर्भर करता है ।

सार्व कुंजी

गुदलेखी यंत्र सामग्री के कुछ तंत्र, गुप्त-सहमाजन प्रक्रिया के जरिए आर्मिंग की अपेक्षा करते हैं और यह अपेक्षा भी करते हैं कि इन सहमाजनों का अंतिम भाग यंत्र सामग्री के साथ इसे आर्म्ड बनाए रखने के लिए, भएतिक रूप से जुड़ा रहे । इस मामले में 'सार्व कुंजी' इस अंतिम सहमाजन को निर्दिष्ट करती है । चूंकि यह निरंतर किसी एक व्यक्ति के कब्जे में नहीं रहती है इसलिए इसे गुप्त नहीं माना जाता ।

संचार / नेटवर्क तंत्र

संबद्ध दूरस्थित जुड़ी युक्तियों और संचार प्रसुविधाओं का, जिनमें एक से अधिक कंप्यूटर तंत्र सम्मिलित हैं, एक ऐसा समुच्चय जिनमें संचार प्रसुविधाओं के माध्यम से, एक-दूसरे के बीच आंकड़े संचरण करने की सामर्थ्य है (आई एस डी एन, लीज लाइनें, डायल-अप, एल ए एन., डब्ल्यू ए एन आदि इसके अंतर्गत आते हैं)

मध्यमार्ग

किसी सुरक्षा नीति का कोई ऐसा उल्लंघन (या संदिध्य उल्लंघन) जिसमें किसी संवेदनशील सुचना का अप्राधिकृत प्रकटीकरण या उस पर नियंत्रण का हास हो सकेगा (सी एफ आंकड़ा इंटिग्रिटी)।

कंप्यूटर

ऐसी कोई इलेक्ट्रॉनिक, चुंबकीय, प्रकाशिक या अन्य तीव्र गति आंकड़ा प्रसंस्करण युक्त या त्र, जो इलेक्ट्रॉनिक, चुंबकीय या प्रकाशिक आवेग के प्रकलन द्वारा तर्कसंगत, गणितीय और स्मृति फलन करता है और इसमें ऐसी सभी निवेश, निर्गम, प्रसंस्करण, भंडारण, कंप्यूटर प्रक्रिया सामग्री या संचार प्रसुविधाएं सम्मिलित हैं, जो कंप्यूटर तंत्र या कंप्यूटर जालक्रम में कंप्यूटर से जुड़े हैं या संबद्ध हैं ।

कंप्यूटर केन्द्र (डाटा केन्द्र देखिए)

कंप्यूटर डाटा संचय

कंप्यूटर आंकड़ा संचय से सूचना, जानकारी, तथ्यों, संकल्पनाओं या अनुदेशों का पाठ, प्रतिबंब, श्रव्य, विडियो में ऐसी समाकृतियां अभिप्रेत हैं जो निश्चित रीति में तैयार किए जा रहे हैं या किए जा चुके हैं या जो किसी कंप्यूटर, कंप्यूटर तंत्र या कंप्यूटर नेटवर्क द्वारा निर्मित किए जा चुके हैं और किसी कंप्यूटर, कंप्यूटर तंत्र या कंप्यूटर नेटवर्क में प्रयोग के लिए आशयित हैं ।

कंप्यूटर नेटवर्क

निम्नलिखित की मार्फत् एक या अधिक कंप्यूटरों का अंतःसंबंधन—

- (i) सेटेलाइट, माइक्रोवेव, ट्रेस्ट्रिमल लाइन या अन्य संसूचना भीड़िया का उपयोग ; और
- (ii) टर्मिनल या कोई काम्पलेक्स जिसमें दो या अधिक अंतःसंबंधित कंप्यूटर हों, चाहे अंतःसंबंधन लगातार बनाए रखा गया हो या नहीं ।

कंप्यूटर पैरीफिरल

साधन उपकरण जो किसी कंप्यूटर के संयोजन से कार्ब करता हो किंतु वह मुख्य कंप्यूटर का ही कोई भाग न हो, जैसे, प्रिन्टर, चुंबकीय टेप रीडर आदि ।

कंप्यूटर संसाधन

साधन कंप्यूटर, कंप्यूटर प्रणाली, कंप्यूटर नेटवर्क, डाटा, कंप्यूटर टाडा बेस या साफ्टवेयर ।

कंप्यूटर प्रणाली

कोई युक्ति या युक्तियों का संग्रहण जिसके अंतर्गत निवेश और निर्गम आधार युक्तियां हैं और जिसमें संगणक नहीं हैं जो कार्यक्रमण योग्य या बाह्य फाइलों के संयोजन के साथ उपयोग किए जाने के योग्य नहीं हैं जिनमें कंप्यूटर कार्यक्रमण, इलैक्ट्रॉनिक अनुदेशक निवेश डाटा और निर्गम डाटा हैं जो लोजिक, अंकगणितीय डाटा भंडारण और पुनःप्राप्ति संसूचना नियंत्रण और कृत्य करते हैं ।

कंप्यूटर वायरस (वायरस देखिए)

विश्वसनीयता

ऐसी अवस्था जिसमें संवेदनशील आंकड़े गुप्त रखे जाते हैं और केवल प्राधिकृत अभिकर्ता को ही प्रकट किए जाते हैं ।

पुष्टि करना

समुचित जांच और अन्वेषण करके सुनिश्चित करना (अधिप्रमाणन भी देखिए : कोई अकीय चिह्न सत्यापित करें)

अंकीय चिह्नक प्रमाणपत्र श्रृंखला की पुष्टि

अंकीय चिह्नक प्रमाणपत्र श्रृंखला अभिपुष्ट करने और अनुवर्ती अंतिम उपयोक्ता ग्राहक अकीय चिह्नक प्रमाणपत्र अभिपुष्ट करने की प्रक्रिया ।

आसंग रेखाचित्र

आयात अनुक्रिया की स्थापना, पूर्तिकर संक्रिया और धंसेतर पुनःप्राप्ति प्रक्रियाएं जो सूचना प्रसंस्करण सुविधा द्वारा या किसी सूचना पद्धति के लिए अनुरक्षित हों ।

सूचना प्रसंस्करण संक्रिया के अभियोजित विघटन से पुनःप्राप्ति के लिए कौशल की स्थापना । कौशल के अंतर्गत पहचान और क्या अवश्य किया जाना चाहिए इसकी पूर्विकता, अपेक्षित कार्रवाई कौन करता है और कौन से औजारों का अवश्य उपयोग किया जाए ।

दस्तावेज जिसका विकास अनुप्रयोग स्वामियों के साथ सर्वनिष्ट किया गया है और प्राथमिक और पूर्तिकर कंप्यूटर अधिष्ठापन से अनुरक्षित किया गया है जो प्रक्रिया बताता है और असामान्य परिस्थितियों जैसे कि धंस के उत्तर में आवश्यक कर्मचारिवृन्द की पहचान करता है । आसंग रेखाचित्र प्रबंधकों को यह सुनिश्चित करने में सहायता करते हैं कि कंप्यूटर अनुप्रयोग स्वामी (कंप्यूटर सहित या रहित) संकटपूर्ण मिशन अनुप्रयोग प्रक्रिया ऐसी दशा में जारी रखे हुए हैं जबकि कंप्यूटर अवलंब अवरुद्ध हो गया है ।

नियंत्रण

किसी प्रक्रिया की अक्षतता और गुणवत्ता सुनिश्चित करने के लिए किए गए उपाय ।

संगतता

एक ही कुंजी युग्म से संबंधित (लोक कुंजी, प्राइवेट कुंजी भी देखें)

अपसामान्य सूचना

डाटा के स्वामी द्वारा, संकटपूर्ण मिशन या कारबार प्रयोजनों के त्वरित आवश्यकता के रूप में निर्धारित डाटा ।

क्रास प्रमाणपत्र

दो प्रमाणन प्राधिकारियों के बीच न्यास संबंध की स्थापना के लिए उपयोग किए जाने वाला प्रमाणपत्र ।

गूढालेखी अलोगरिधम

अभिकलन के लिए स्पष्ट रूप से विनिर्दिष्ट गणितीय प्रक्रिया, नियमों का ऐसा विहित समुच्चय जो विहित परिणाम देता है।

गूढालेखी (लोक कुंजी गूढालेखी भी देखिए)

(i) डाटा को ऐसे परिवर्तित आरूप में प्रतिस्थापित करके, जिसे किसी ऐसे व्यक्ति द्वारा, जो समुचित गूढालेखी अलोगरिधम और कुंजी धारण करता है, मूल डाटा के प्रकटीकरण के लिए पुनःपरिवर्तित किया जा सकता है, उनकी गोपनीयता और अधिग्राहण को सुनिश्चित करने के लिए प्रयुक्त गणितीय विज्ञान।

(ii) डाटा को, उनकी सूचना अंतर्वस्तु छुपाने, उनमें अनभिज्ञात रूप से रूपांतरण और / या उनके अप्राधिकृत उपयोगों को रोकने के लिए डाटा परिवर्तित करने के लिए ऐसा कोई डिस्प्लिन जो सिद्धान्तों, उपायों और ढंग को सम्मिलित करता है।

नुकसान से, किसी कंप्यूटर साधन को किसी उपाय से नष्ट, परिवर्तित, विलोप, परिवर्धन, रूपांतरण या पुनःक्रमांकित करना अभिप्रेत है।

डाटा

डाटा से सूचना, जानकारी, तथ्यों, संकल्पनाओं या अनुदेशों की ऐसी समाकृतियां अभिप्रेत हैं जिन्हें निश्चित रीति से तैयार किया जा रहा है या किया गया है और किसी कंप्यूटर तंत्र या कंप्यूटर नेटवर्क में प्रसंस्करण के लिए आशयित हैं। प्रसंस्कृत की जा रही है या प्रसंस्कृत की गई हैं और जो किसी भी रूप (जिसमें कंप्यूटर मुद्रित पृष्ठ, चुंबकीय या प्रकाशिक भंडारण मीडिया, छिद्रित पत्रक, छिद्रित टेप सम्मिलित हैं) में हो सकेंगी या जिन्हें कंप्यूटर की स्मृति में अंतरिक रूप से भंडारित किया जा सकेगा।

डाटा संचय (कंप्यूटर डाटा संचय देखिए)

डाटा केन्द्र (जैसा कि कंप्यूटर केन्द्र भी है)

ऐसी प्रसुविधा जिसके अंतर्गत कंप्यूटर कक्ष, मीडिया पुस्तकालय, नेटवर्क क्षेत्र, सर्वर क्षेत्र, क्रमादेशन तथा प्रशासन क्षेत्र, अन्य भंडारण और कंप्यूटर प्रसंस्करण फलनवों को करने के लिए प्रयुक्त आलंब क्षेत्र आते हैं। यह अधिकांशतः कंप्यूटर कक्ष और मीडिया पुस्तकालय को निर्दिष्ट करता है।

डाटा गोपनीयता (गोपनीयता देखिए)

डाटा इंटिग्रिटी

डाटा इंटिग्रिटी एक ऐसी स्थिति है जिसमें डाटा को अप्राधिकृत रूप से न ही बदला गया हो और न हो नष्ट किया गया हो (कृपया देखिए धोट ; कंप्रोमाइज)

डाटा सुरक्षा

डाटा को दुर्घटनावश या मैलिसियस रूपांतरण, नष्ट करने या प्रकटन से रोकने की प्रथा।

प्रदर्शन प्रमाणपत्र

प्रमाणन प्राधिकारी द्वारा प्रदर्शन और प्रस्तुतीकरण के प्रयोजनों के लिए और न कि किसी सुरक्षित या गोपनीय संचार के लिए जारी किया गया अंकीय चिह्नक प्रमाणपत्र। प्रदर्शन अंकीय चिह्नक प्रमाणपत्रों का प्रयोग प्राधिकृत व्यक्तियों द्वारा ही किया जा सकेगा।

अंकीय प्रमाणपत्र आवेदक

एक ऐसा व्यक्ति जो सार्वजनिक की अंकीय चिह्नक प्रमाणपत्र जारी करने के लिए प्रमाणन प्राधिकारी से अनुरोध करता है (कृपया सी.ए. आवेदक : सबस्क्राइबर देखें)

अंकीय प्रमाणपत्र उपयोजन

अंकीय चिह्नक प्रमाणपत्र आवेदक से प्रमाणन प्राधिकरी को अंकीय चिह्नांकन प्रमाणपत्र जारी करने के लिए अनुरोध (कृपया प्रमाणपत्र आवेदक : प्रमाणपत्र चिह्नांकन, अनुरोध)

अंकीय चिह्नक

इससे इलैक्ट्रानिक विधि या प्रक्रिया से सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 3 के उपबंधों के अनुसरण में इलैक्ट्रानिक अभिलेख का अधिप्रमाणन अभिप्रेत है।

अंकीय चिह्नक प्रमाणपत्र

इससे सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 35 की उपधारा (4) के अधीन जारी अंकीय चिह्नक प्रमाणपत्र अभिप्रेत है।

विशिष्ट नाम

विशिष्ट नाम से वास्तविक विश्व में विद्यमान निकाय जैसे कि कंप्यूटर आधारित परिप्रेक्ष में कोई व्यक्ति अभिप्रेत है।

दस्तावेज

दस्तावेज से अभिलेख अभिप्रेत हैं जिसमें मूर्त माध्यम जैसे कि कागज पर अलिखित सूचना सम्मिलित है न कि कंप्यूटर आधारित सूचना। (कृपया देखें संदेश : अभिलेख)

इलैक्ट्रानिकी रूप

सूचना के संदर्भ में इससे भीड़िया, मैग्नेटिक, प्रकाशकीय, कंप्यूटर मैमोरी, माइक्रोफिल, कंप्यूटर सृजित माइक्रोफिसे या ऐसी ही युक्तियों पर किसी सूचना का सृजन भेजा जाना प्राप्त करना या भंडारण अभिप्रेत है।

इलैक्ट्रानिक मेल ("ई-मेल")

कंप्यूटर आधारित संचार तंत्र के माध्यम से संदेशों का भेजना, प्राप्त करना या अग्रेषण अभिप्रेत है।

इलैक्ट्रानिक अभिलेख

इलैक्ट्रानिकी प्ररूप या माइक्रोफिल्म या कंप्यूटर सृजित माइक्रोफिसे के माध्यम से प्राप्त या भेजे गए डाटा अभिलेख या सृजित डाटा इमेज या भंडारित ध्वनि अभिप्रेत है।

कूटकरण

आम डाटा को अमूर्त प्ररूप (बीजलेख पाठ) में परिवर्तन की प्रक्रिया ताकि मूल डाटा की या तो पुनः प्राप्ति (एक तरफा कूटकरण) या उसे विपरीत पुनः कूटकरण प्रक्रिया के बिना प्राप्त न किया जा सके (दो तरफा कूटकरण) की प्रक्रिया।

विस्तार

एक्स. 509 वी३ प्रमाणपत्रों में विस्तार क्षेत्र (कृपया देखे एक्स 509)।

फायर वाल /दोहरी फायर वाल

ये अनेक बुद्धिमान युक्तियों में से एक हैं जो नेटवर्कों को अलग करने के काम में आती हैं (जैसे कि राउटर या गेटवे)। फायर वाल आक्रमणकारियों का एक नेटवर्क से दूसरे नेटवर्क में जाना नुश्चिकल जरूरी है। दोहरा फायर वाल से आपस में जुँड़ी हुई दो फायर वाल अभिप्रेत हैं। दोहरी फायर वाल लक्ष जाहिन को कम करती है जिसमें एक फायर वाल पर काबू कर लिया जाता है या जिससे एड्रेस ट्रान्सलेशन कृत्य उपलब्ध हो जाता है।

फाइल अंतरण प्रोटोकॉल (एफ.टी.पी.)

एक अनुप्रयोग प्रोटोकॉल जो इंटरनेट सूट या प्रोटोकॉल से फाइल प्रणाली एक्सेस उपलब्ध करता है।

कृत्य

कंप्यूटर के संबंध में इससे कंप्यूटर से या कंप्यूटर में लॉजिक नियंत्रण अंकगणितीय प्रक्रिया विलोपन, भंडारण और पुनः प्राप्ति तथा संचार और दूर संचार सम्मिलित हैं।

गेट वे

गेट वे से हार्डवेयर अथवा शाफ्टवेयर अभिप्रेत है जो दो या अधिक प्रणालियों के बीच प्रोटोकॉल को ट्रान्सलेट करने के प्रयोग में आता है।

कुंजी युग्म का सृजन

अंकीय हस्ताक्षर प्रमाणन आवेदन के समय निजी की सृजित करने की एक विश्वनीय प्रक्रिया जिनकी तदनुरूपी सार्वजनिक कुंजी अंकीय चिह्नक प्रमाणन आवेदन के दौरान प्रमाणन प्राधिकारी को ऐसी रीति से प्रस्तुत की गई थी जिनसे आवेदक की प्राइवेट कुंजी को इस्तेमाल करने की हैसियत का प्रदर्शन होता है।

हार्ड कापी

हार्ड कापी से कंप्यूटर का आउटपुट अभिप्रेत है जो कि कागज पर पढ़े जा सकने वाले रूप में हो अर्थात् मुद्रित रिपोर्ट सूचियां और दस्तावेज़।

हैश (हैश कृत्य)

एल्गोरिदम जो बिट के एक सेट को (सामान्यतः छोटे) सेट में इस प्रकार से परिवर्तित करती है जिससे कि :

- (i) कोई संदेश प्रत्येक समय वही परिणाम देता है जिस समय उसी संदेश को इनपुट के रूप में इस्तेमाल करते हुए एल्गोरिदम को निष्पादित किया गया था।
- (ii) संगणनीय रूप से किसी संदेश का एल्गोरिदम द्वारा प्रस्तुत परिणाम से पुनर्निर्माण संभव नहीं हो।
- (iii) दो विभिन्न संदेशों के लिए समान एल्गोरिदम का प्रयोग करके समान हैश परिणाम संगणनीय रूप से देना संभव न हो।

उच्च सुरक्षा जोन

एक ऐसा क्षेत्र जिसमें एक्सेस प्रवेश बिन्दु से नियंत्रित हो और जो समुचित रूप से परखे गए व्यक्तियों और उचित रूप से संरक्षित आगंतुकों तक सीमित हो। उच्च सुरक्षा जोन तक पहुंच केवल सुरक्षा जोन से ही होनी चाहिए और उन्हें सुरक्षा जोनों और प्रचालन जोनों से किसी पैरामीटर के माध्यम से अलग किया गया हो। उच्च सुरक्षा जोनों को प्रत्येक दिन चौबीस घंटे, प्रत्येक सप्ताह सुरक्षा कार्मिकों, अन्य व्यक्तियों या इलेक्ट्रॉनिकी माध्यम से मानीटर किया जाना चाहिए।

पहचान/पहचान करना

किसी व्यक्ति की पहचान का सुनिश्चय करने की प्रक्रिया पब्लिक की क्रिप्टोग्राफी में प्रमाणपत्रों के माध्यम से शिनारख में सहायता की जाती है।

पहचान

एक विशिष्ट सूचना जिससे किसी डोमेन के भीतर किसी विशिष्ट प्रविष्टि का पता चलता है। ऐसी सूचना किसी विशिष्ट डोमेन में ही विशेष होती है।

सूचना

इसमें डाटा डेक्स्टर इमेज, ध्वनि, आवाज, कोड, कंप्यूटर प्रोग्राम साफ्टवेयर और डाटा केन्द्र अथवा प्रारूपित या कंप्यूटर सृजित माइक्रोफिसे सम्मेलित हैं।

सूचना आस्तियां

सूचना आस्तियों से किसी कारबार के दौरान इस्तेमाल किए गए सूचना स्रोत अभिप्रेत हैं और इसमें सभी सूचना अनुप्रयोग शाफ्टवेयर (विकसित या क्रय किए हुए), और प्रौद्योगिकी (हार्डवेयर प्रणाली, शाफ्टवेयर और नेटवर्क सम्मिलित हैं) ।

इंटरमीडिएटरी

किसी विशेष इलेक्ट्रॉनिकी संदेश के संदर्भ में इससे कोई व्यक्ति जो किसी और व्यक्ति की ओर से उस संदेश को अभिप्राप्त करता है, का भंडारण करता है या सप्रेषित करता है या उस संदेश के संबंध में कोई सेवा प्रदान करता है, अभिप्रेत है ।

सुरक्षा प्रौद्योगिकी सुरक्षा

गोपनीयता, सत्यनिष्ठा, प्राप्यता, जवाबदारी, अधिप्रमाणिकता और विश्वसनीयता को परिमापित, प्राप्त करने और बनाए रखने संबंधी सभी पहलू ।

सूचना प्रौद्योगिकी सुरक्षा नीति

नियम, निदेश और पद्धतियां, जो किसी संगठन और उसके सूचना प्रौद्योगिकी तंत्र के भीतर सूचना आस्तियां जिसके अंतर्गत संवेदी सूचना है किस प्रकार प्रबंधित, संरक्षित और वितरित की जाती है इनको, शासित करती हैं ।

कुंजी

संकेतों का अनुक्रम जो गूढ़लेखी रूपान्तरण के प्रचालन के नियंत्रित करता है (अर्थात् कुट्टलेख, प्रतिकूट्टलेख, गूढ़लेखी जांच फलन गणन, चिन्हक उत्पादन या चिन्हक सत्यापन) ।

कुंजी उत्पादन

प्राइवेट कुंजी/लोक कुंजी सर्जित करने की विश्वास योग्य प्रक्रिया ।

कुंजी प्रबंधन

सुरक्षा नीति के अनुसार कुंजीकरण सामग्री के उत्पादन, रजिस्ट्रीकरण, प्रमाणीकरण, रजिस्ट्रीकरण हटाने, वितरण, प्रतिष्ठापन, भंडारण, अभिलेखकरण, प्रतिसंहरण, व्युत्पत्ति और धंस का प्रबंधन और उपयोग ।

कुंजी गुप्त

असमिति गुप्त तंत्र में अभिप्रेत है प्राइवेट कुंजी और इसकी गणितीय ढंग से संबंधित लोक कुंजी, जो इस प्रकार संबंधित है कि लोक कुंजी प्राइवेट कुंजी द्वारा सर्जित किसी अकीय चिन्हक को सत्यापित कर सकती हैं ।

अनुज्ञाप्ति

से अभिप्रेत है प्रमाणीकरण प्राधिकारी को मंजूर की गई अनुज्ञाप्ति ।

स्थानीय क्षेत्र नेटवर्क (एल ए एन)

किसी समूह या विभाग द्वारा संबद्ध प्रक्रिया सामग्री और यंत्र सामग्री स्रोतों को बांटने में प्रयोग किए गए कंप्यूटरों और सहायक घटकों का भौगोलिक रूप से लघु नेटवर्क ।

अ-संवेदी

ऐसी सूचना को लागू होता जो, यदि जोखिम में उठाया जाए, उपयुक्त रूप से राष्ट्रीय हित से बाहर क्षति कारित करने की प्रत्याशा की जा सकती है, उदाहरणार्थ, वास्तविक वेतन को प्रकट करना ।

अंकीय चिन्हक प्रमाणपत्र

(प्रमाणपत्र प्रबंधन देखिए)

मीडिया

सामग्री या समाकृति जिस पर आंकड़े अभिलिखित किए जाते हैं। उदाहरण के अंतर्गत चुंबकीय टेप और डिस्क हैं।

संदेश

सूचना का अंकीय प्रतिरूप; कंप्यूटर आधारित अभिलेख। अभिलेख का उपसमुच्चय (अभिलेख भी देखें)

नाम

कतिपय प्रकार की किसी सत्ता का वर्णन करने के लिए तात्परित परिचायक प्रतीकों का समुच्चय।

नेटवर्क

संबंधित, दूरस्थ संयोजित युक्तियां और संचार सुविधाएं जिनके अंतर्गत संचार सुविधाओं के माध्यम से उनमें डाटा प्रेषित करने के सामर्थ्य वाले एक से अधिक कंप्यूटर तंत्र हैं।

नेटवर्क प्रशासक

कंप्यूटर नेटवर्क प्रतिष्ठापन का कोई व्यक्ति जो डिजाइन करता है। नियंत्रण करता है और कंप्यूटर नेटवर्क का उपयोग करता है।

उलझान

किसी नेटवर्क में बिंदु जिस पर एक से अधिक फलन इकाईयां प्रणाल या डाटा सर्किटों को जोड़ देती हैं।

नामनिर्देशित वेबसाईट

प्रमाणेकरण प्राधिकारी द्वारा सूचना के प्रदर्शन के लिए नामित वेबसाईट जैसे कि फीस की सूची, प्रमाणन प्रक्रिया विवरण, प्रमाणपत्र नीति आदि।

खंडनेतर

प्रेषक के संरक्षण के अनुक्रम में डाटा के उद्भव या परिदान के संरक्षण की बाबत प्राप्तकर्ता द्वारा कोई झूठा प्रत्याख्यान करने के विरुद्ध सबूत का उपबंध करता है कि प्रेषक द्वारा झूठा प्रत्याख्यान करने वाले के विरुद्ध प्राप्तिकर्ता द्वारा डाटा प्राप्त किया गया है या उसका संरक्षण किया गया है कि प्रेषक द्वारा डाटा वस्तुतः भेजा गया है। टिप्पणी : केवल तथ्य का कोई प्रयासकर्ता (जिसमें विवादों का समाधान करने वाला प्राधिकारी भी है) खंडनेतर का अंततोगत्वा अवधारण कर सकता है। उदाहरणार्थ इस प्रमाणन प्रक्रिया विवरण के परिणामस्वरूप सत्यापित अंकीय चिन्हक का किसी तथ्य के प्रयासकर्ता द्वारा खंडनेतर अवधारण के समर्थन में सबूत का उपबंध कर सकता है। किंतु स्वतः खंडनेतर कार्य नहीं कर सकता है।

नोटरी

किसी कार्यपालिक शासकीय अधिकरण द्वारा नोटरी सेवाओं को, अर्थात् अभिस्वीकृति लेने, शपथ दिलाने और प्रतिज्ञान करने, चिन्हक साक्षायित करने या सत्यापित करने और परक्राम्य लिखतों पर प्रतिवादों पर टिप्पणी आधि, संपादित करने के लिए प्राधिकृत किया गया कोई प्राकृत व्यक्ति।

युगपत

सघ अनुक्रिया संबंधन का उपबंध करने वाला संचार।

संक्रिया क्षेत्र

वह क्षेत्र जहां अभिगम वहां काम करने वाले कर्मचारिवृन्द और उचित रीति से मार्गरक्षित आगंतुकों तक सीमित है। समय-समय पर आशंका की जोखिम निर्धारण (टी आर ए) पर आधारित संक्रिया क्षेत्र, कम-से-कम, मानिटर किए जाने चाहिए और अधिमानतः उक्त निर्धारण अभिग्रहण क्षेत्र से किए जाने चाहिए।

संक्रियात्मक प्रमाणपत्र

ऐसा अंकीय चिन्हक प्रमाणपत्र जो विद्यमान तारीख और समय पर या किसी भिन्न विनिर्दिष्ट तारीख और समय पर, संदर्भ के अनुसार, अपनी संक्रियात्मक अवधि के भीतर है।

संक्रियात्मक प्रबंधन

सभी कारबार/सेवा इकाई प्रबंधन (अर्थात् उपयोक्ता प्रबंधन) के साथ-साथ सूचना प्रौद्योगिकी प्रबंधन के प्रति निर्देश करता है।

संक्रियात्मक अवधि

किसी अंकीय चिन्हक प्रमाणपत्र के जारी होने की तारीख और समय से (या किसी पश्चात्वर्ती तारीख और समय पर निश्चित यदि अंकीय चिन्हक प्रमाणपत्र में बताया जाए) आरंभ होकर तथा उस तारीख और समय के साथ समाप्त होती है कि अंकीय चिन्हक प्रमाणपत्र का समापन होता है या इसके पूर्व निलिपि या प्रतिसंहित किया जाए।

संगठन

ऐसी ईकाई जिसके साथ कोई उपयोक्ता का संबंधन होता है। संगठन कोई उपयोक्ता भी हो सकता है।

प्रवर्तक

वह व्यक्ति जो इलैक्ट्रोनिक संदेश भेजता है, उत्पादित करता है, भंडारण करता है या प्रेषित करता है अथवा किसी :अन्य व्यक्ति को इलैक्ट्रोनिक संदेश भेजना, उत्पादित करना, भंडारित करना या प्रेषित करना कारित करता हैं लेकिन इसके अंतर्गत कोई मध्यस्थ नहीं है।

पहचान शब्द (पहचान वाक्यांश ; पिन संख्यांक)

गोपनीय प्रभानन सूचना जो कि प्रायः कंप्यूटर साधन के लिए अभिगम का उपबंध करने के लिए प्रयुक्त रज्जु प्रतीकों को संघटित करती है।

विशिष्टतः संदर्भी

ऐसी सूचना पर लागू होती है जो, यदि जोखिम हो तो पर्याप्त रूप से राष्ट्रीय हितों से बाहर गंभीर क्षति कारित करने रज्ञात्यता होती है, उदाहरणार्थ ख्याति या प्रतियोगी उत्कर्ष की हानि।

पी सी कार्ड (स्मार्ट कार्ड भी देखें)

पर्सनल कंप्यूटर मेमौरी कार्ड इंटरनेशनल एसोसिएशन (पी सी एम सी आई ए) द्वारा प्रख्यापित मानकों के अनुसार यंत्र :सामग्री टोकन जो कंप्यूटर की क्षमता में वृद्धि का उपबंध करता है, जिसके अंतर्गत सूचना सुरक्षा का सरलीकरण भी है।

व्यक्ति

से वर्गीकृत कंपनी या संगम या व्यष्टि या व्यष्टियों का निकाय अभिप्रेत है, वह निर्गमित हो या अनिर्गमित।

वैयाक्तिक उपायिति

प्रमाणन प्राधिकारी या उसके पदाधिकारी के समझ उपसंजात होने (स्वयं या वास्तविक रूप से अंकीय रूप से) और कतिपय परिस्थितियों के अधीन अंकीय चिन्हक प्रमाणपत्र के लिए पूर्व अपेक्षा के रूप में एक पहचान को साबित करने का कार्य।

लोक कुंजी अवसंरचना/लोक कुंजी अवसंरचना सर्वर

अंकीय चिन्हक प्रमाणपत्रों और पब्लिक-प्राइवेट कुंजी युग्म की व्यवस्था करने के प्रयोजन के लिए प्रयुक्त पालिसियों ; प्रक्रियाओं ; सर्वर प्लेटफार्म सफ्टवेयर और कार्यक्रमों ; जिसके अंतर्गत लोक कुंजी प्रमाणपत्रों को जेनरेट करने, उनको जारी करने, उनका रखरखाव करने और उनके प्रतिसंहित करना भी सम्मिलित है, के एक सेट।

लोक कुंजी अवसंरचना उत्क्रम

ऐसे प्रमाणन प्राधिकारियों का एक सेट जिनके कृत्य प्राधिकरण के प्रत्यायोजन के सिद्धांतों के अनुसार संगठित किए जाते हैं और जो अधीनस्थ और वरिष्ठ प्रमाणन प्राधिकारी के रूप में प्रत्येक अन्य से संबंधित हैं।

गिरवी (साफ्टवेयर प्रकाशकों की गिरवी)

नीति

एक संक्षिप्त दस्तावेज जो उच्च-स्तरीय संगठनात्मक हैसियत विस्तार को कथित करता है और ऐसे व्यक्ति को सुव्यवस्थित करता है जो नीति और तत्पात्रीय मानकों का पालन करने के लिए जिम्मेदार है।

निम्नलिखित संक्षेपाक्षर इस बात के उदाहरण है कि नीति में क्या अंतर्विष्ट है :—

- प्रस्तावना
- परिमाणाएं
- “विषय वस्तु” (अर्थात् आंकड़े प्रतिभूति) की आवश्यकता को पहचानने के लिए नीति पूरक कथन
- विस्तार क्षेत्र
- लोगों की भूमिका और उनकी जिम्मेदारी
- प्रवर्तन, जिसमें जिम्मेदारी भी है, संबंधी कथन

प्राइवेट कुंजी

अंकीय चिन्हक सृजित करने के लिए उपयुक्त युग्म कुंजी की कुंजी।

प्रक्रिया

यह सुनिश्चित करने के लिए मार्गदर्शी सिद्धांतों की पूर्ति कर ली गई है, निष्पादित उपायों का एक सेट।

कार्यक्रम

कुछ प्रयोजनों को पूरा करने के लिए एक विस्तृत और स्पष्ट अनुदेशों का सेट, कंप्यूटर के निवेश के लिए या मशीनीकरण में उपयुक्त कठिपय भाषा को अभिव्यक्त करने वाला सेट।

परोक्षी सर्वर

ऐसा सर्वर जो क्लाइंट एप्लीकेशन जैसे बेव ब्रोजर और रियल सर्वर के बीच है। यह उन अनुरोधों को रियल सर्वर को यह देखने के लिए अभिग्रहण करता है कि क्या वह स्वयं इस अनुरोध को पूरा करने में समर्थ है। यदि नहीं, तो वह रियल सर्वर को यह अनुरोध भेज देता है।

पब्लिक एक्सेस जोन

साधारणतः सराउंड या फार्मर्स सरकारी प्रसुविधा के भाग है। उदाहरणार्थ इसके अंतर्गत किसी भवन की सराउंडिंग के ग्राउंड्स और पब्लिक कौरीडोर और बहुभौगी भवनों में एलीवेटर लाबीज सम्मिलित है। सीमा निर्धारक, जैसे संकेत और दिशा या रिमोट (दूरस्थ) निगरानी, अप्राधिकृत क्रियाकलापों को हतोत्साहित करने में उपयोग किया जा सके।

लोक कुंजी

अंकीय चिन्हक के सत्यापन और अंकीय चिन्हक प्रमाणपत्र को सूचीबद्ध करने के लिए उपयोग किया जाने वाली कुंजी युग्म की कुंजी।

लोककुंजी प्रमाणपत्र (प्रमाणपत्र देखिए)

लोक कुंजी क्रिप्टोग्राफी (देखिए क्रिप्टोग्राफी)

क्रिप्टोग्राफी का एक प्रकार, जिसका क्रिप्टोग्राफी कुंजी से संबंधित अंकगणितीय की युग्म के लिए उपयोग किया जाता है। लोक कुंजी किसी ऐसे व्यक्ति को उपलब्ध कराई जा सकेगी जो उसका उपयोग करना चाहे और सूचना को इंक्रिप्ट कर सकेगा या अंकीय चिन्हक को सत्यापित कर सकेगा; प्राइवेट कुंजी को उसके धारक को गुप्त रूप से रखा जाता है और जो सूचना डिक्रिप्ट कर सकेगा या अंकीय चिन्हक को सुजित कर सकेगा।

लोक कुंजी अवसंरचना

आर्किटेक्चर, संगठन, तकनीकी, प्रेक्टिसेस और प्रक्रियाएं जो सामूहिक रूप से पब्लिक की क्रिप्टोग्राफिक पद्धति पर आधारित प्रमाणपत्र को कार्यान्वयन करने में और उसके प्रचालन सहायक है इसमें सुव्यवस्थित अंकीय चिन्हक प्रमाणपत्र और कीज़ के प्रयोजन के लिए प्रयुक्त नीतियाँ, प्रक्रियाओं, सर्वर प्लेटफार्मों, साफ्टवेयर और कार्य केन्द्र भी सम्मिलित हैं।

लोक/प्राइवेट कुंजी युग्म (लोक कुंजी ; प्राइवेट कुंजी ; कुंजी युग्म देखिए)

प्राप्तिकर्ता

ऐसा व्यक्ति जो अंकीय चिन्हक प्राप्त करता है और जो इस पर विश्वास करने की स्थिति में चाहे ऐसे विश्वास की स्थिति पैदा होती है या नहीं (विश्वास करने वाली पार्टी भी देखिए)

अभिलेख

सूचना यह है जो मूर्त माध्यम (दस्तावेज) में अंतर्लिखित है या इलैक्ट्रॉनिक या अन्य माध्यमों में स्टोर है और उसे पुनर्प्राप्ति के लिए देखा जा सकता है। “रिकार्ड” पद “दस्तावेज” और “संदेश” दो पदों का सुपर सेट है (दस्तावेज ; संदेश भी देखिए)

रिइनरोलमैंट (नवीकरण भी देखिए)

रिले/रिलांयस (किसी प्रमाणपत्र और अंकीय चिन्हक पर)

अंकीय चिन्हक को स्वीकार करना और किसी ऐसी रीति में कार्य करना जो स्वयं के लिए हानिकारक हो सकती जिससे अंकीय चिन्हक को निष्प्रभावी किया जाना था (रिलांयिंग पार्टी ; प्राप्तिकर्ता भी देखिए)।

रिलायिंग पार्टी

ऐसा प्राप्तिकर्ता जो किसी प्रमाणपत्र और अंकीय चिन्हक पर विश्वास करके कार्य करता है (प्राप्तिकर्ता, रिले या रिलांयस भी देखिए) (किसी प्रमाणपत्र और अंकीय चिन्हक पर)।

नवीकरण

नए समाप्त हुए विद्यमान अंकीय चिन्हक प्रमाणपत्र के स्थान पर उसी वर्ग और प्रकार तथा वैसी ही विषय के नए अंकीय चिन्हक प्रमाणपत्र को अभिप्राप्त करने की प्रक्रिया।

रिपोजिटरी

डाटा आधारित अंकीय चिन्हक प्रमाणपत्रों और आन लाइन पर पहुंच योग्य अन्य सुसंगत सूचना।

खंडन (रिप्यूडियेशन) - [मंडन (नान रिप्यूडियेशन) भी देखिए]

अस्तित्व द्वारा किसी बात को प्राप्ताख्यान करने का प्रयास करना जिसमें किसी संसूचना, जो संपूर्णतया या मात्र रूप से जानकारी देती है, भी अंतर्वलित है।

प्रमाणपत्र का प्रतिसंहृष्टण

किसी विनिर्दिष्ट समय से किसी अंकीय विन्हक प्रमाणपत्र की प्रचालन अवधि की स्थायी रूप से समाप्ति की प्रक्रिया ।

जोखिम

ऐसी पद्धति या सहबद्ध आस्तिया जो सुरक्षा आंशका और सुभेदकारी, संयोजन के परिणामस्वरूप होती है, संभावित नुकसान पहुंचाती है ।

जोखिम विश्लेषण

सुरक्षा जोखिमों की पहचान, उनके परिमाण का अवधारण आवश्यक क्षेत्रों के सुरक्षापायों की पहचान की प्रक्रिया ।

जोखिम निर्धारण

प्राक्कलित संभावनाओं पर आधारित कतिपय घटनाएं, जो ऐसी घटनाएं से होती हैं, से संभावित हानि को सुव्यवस्थित करने के लिए आस्ति पद्धति और सुभेदकारी का विश्लेषण ।

जोखिम प्रबंधन

पहचान, नियंत्रण और विलोपन या अनिश्चित घटनाओं को कम करने की कुल प्रक्रिया जो सूचना प्रौद्योगिकी प्रणाली के संसाधनों को प्रभावित कर सकेगी ।

आर.एस.ए.

रिवेस्ट शमीर और अदलमेन ने लोककुंजी गुदालेखी तंडकी खोज की थी ।

गुप्त अंश

भौतिक संकेतों की संख्या में से गूदालेखी गुप्त विभाजन का कोई भाग सुरक्षित प्रणाल (चैनल) संचार पथ में गूदालेखी रूप से बढ़ाया गया जो अनुभवगम्य प्रतिरक्षा के विरुद्ध संदेशों की रक्षा करते हैं ।

सुनिश्चित प्रणाली

से कंप्यूटर यंत्र सामग्री, प्रक्रिया सामग्री और प्रक्रिया अभिप्रेत है जो—

- (क) अप्राधिकृत पहुंच और दुरुपयोग का युक्तियुक्त रूप से सुनिश्चित करता है ;
- (ख) विश्वसनीयता और सही प्रचालन का युक्तियुक्त स्तर प्रदान करता है ;
- (ग) आशयित कृत्यों का पालन करने के लिए युक्तियुक्त रूप से उपयुक्त है ; और
- (घ) समान्य: स्वीकृत प्रतिरक्षा प्रक्रियाओं को स्थिर रखता है ।

सुरक्षा प्रक्रिया

से सूचना प्रौद्योगिकी की अधिनियम, 2000 की धारा 16 के अधीन विहित सुरक्षा प्रक्रिया अभिप्रेत है ।

सुरक्षा

अप्राधिकृत पहुंच या अनियंत्रित हानिया या प्रभाव से सुरक्षित क्वालिटी या अवस्था/आत्यंतिक सुरक्षा व्यवहारिक रूप से प्राप्त करना असंभव है और दी गई सुरक्षा प्रणाली की क्वालिटी आपेक्षित है । राज्य माडल सुरक्षा तंत्र के भीतर “सुरक्षा” विभिन्न प्रचालनों के अधीन अभिरक्षित किए जाने वाला विनिर्दिष्ट “राज्य” है ।

सुरक्षा नीति

कोई दस्तावेज, जो विश्वसनीय प्रणाली द्वारा बनाए रखे गए संरक्षण के संबंध में अपेक्षाओं और अच्छे व्यवहारों के व्यक्त करते हैं ।

सुरक्षा सेवाएं

सुरक्षा संरचना के समुच्चय द्वारा दी गई सेवाएं और कतिपय सुरक्षा यांत्रिकी के साधनों द्वारा निष्पादित ऐसी सेवाओं में पहुंच नियंत्रण, डाटा विश्वसनीयता और डाटा एकीकृत सम्मिलित हैं पर सीमित नहीं।

सुरक्षा जोन

कोई ऐसा क्षेत्र जिसकी पहुंच प्राधिकृत कार्मिक और अनुरक्षण को सीमित करने के लिए/सुरक्षा जोनों को भिन्न प्रचालन जोन में अधिमान्य रूप से पहुंच योग्य और विनिर्दिष्ट प्रवेश बिन्दु से होना चाहिए।

स्वयं चिन्हक लोक कुंजी

आंकड़ा डाटा जिसका उसी अंकीय चिन्हक प्रमाणपत्र के रूप में निर्मित है किन्तु इसमें विषय द्वारा चिन्हित हैं। जब तक अंकीय चिन्हक प्रमाणपत्र, स्वयं चिन्हक लोक कुंजी का प्रयोग अन्य पक्षकारों को लोक कुंजी प्राधिकृत करने के लिए विश्वसनीय रूप से प्रयोग नहीं किया जा सकता है।

क्रम संख्यांक (देखिए क्रम संख्यांक प्रमाणपत्र)

सर्वर

सर्वर प्रणाली जो मुवक्किल प्रणालियों से अनुरोध करने के लिए अनुकूल है।

चिन्हक

संदेश के लिए या दस्तावेज में चिन्हक किए जाने के लिए अंकीय चिन्हक का सृजन करना जो संदर्भ पर निर्भर है।

चिन्ह (अंकीय चिन्हक देखिए)

चिन्हक

कोई व्यक्ति जो संदेश या दस्तावेज के लिए किसी चिन्हक के लिए अंकीय चिन्हक का सृजन करता है।

चुस्त कार्ड

हार्डवेयर रोकन जो एक या अधिक एकीकृत परिपथ (ए.प.) चिपों को गूढ़ालेखी कृत्यों के क्रियान्वयन के लिए नियंत्रित करता है और जो आकर्षित करने के लिए अंतर्निहित प्रतिरोध को रखता है।

एस/माइन

किसी इंटरनेट माइन पर्यावरण में गूढ़ालेखी संदेश संश्लेष उपयोग ई-मेल सुरक्षा के लिए विनिर्देश।

विषय (प्रमाणपत्र का)

लोक कुंजी के तत्स्थानी प्राइवेट कुंजी का धारक। “विषय” पद उपस्कर या युक्ति दोनों को निर्दिष्ट करता है जो प्राइवेट कुंजी धारित करता है उस व्यक्तिको, यदि कोई है। जो उस उपस्कर या युक्ति को नियंत्रित करता है। विषय असंदिग्ध नाम को समनुदेशित है जो विषय के अंकीय चिन्हक प्रमाणपत्र में अंतर्विष्ट लोक कुंजी को बाध्य हो।

विषय नाम

विषय नाम में सुस्पष्ट मूल्य अंकीय चिन्हक प्रमाणपत्र का क्षेत्र जो लोक कुंजी को बाध्य है।

अभिदाता

कोई ऐसा व्यक्ति, जिसके नाम में अंकीय चिन्हक प्रमाणपत्र जारी किया गया है।

अभिदाता करार

इस प्रमाणन व्यवहार विवरण के अनुसार पदाभिहित लोक प्रमाणन सेवाओं के उपबंध के लिए अभिदाता और प्रमाणकर्ता प्राधिकारी के बीच निष्पादित करार।

अभिदाता सूचना

अंकीय चिन्हक प्रमाणपत्र आवेदन (आवेदन प्रमाणपत्र भी देखिए) के भाग के रूप में प्रमाणन प्राधिकारी को प्रदान की गई सूचना ।

प्रमाणपत्र निलंबन

अंकीय चिन्हक प्रमाणपत्र के स्थायी प्रतिसंहरण के बिना अंकीय चिन्हक प्रमाणपत्र की प्रचालन अवधि प्रभाव पर अस्थायी “धारण” रखा गया है । अंकीय चिन्हक प्रमाणपत्र निलंबन अर्थात् कारण कोड केच साथ सी आर एल प्रविष्टि द्वारा किया गया है ।

(प्रतिसंहरण प्रमाणपत्र भी देखिए)

तंत्र प्रशासनि

कंप्यूटर संस्थापन पर कोई ऐसा व्यक्ति जो कंप्यूटर तंत्र को डिजाइन करता है, नियंत्रित करता है और प्रबंध करता है ।

तंत्र सुरक्षा

तंत्र के कृत्य जो कतिपय उपयोक्ताओं को वस्तुओं के प्रयोग करने से निर्बंधित करता है ।

साफ्टवेयर तंत्र

आवेदन आत्मनिर्भर साफ्टवेयर जो उपयोजन प्रक्रिया सामग्री को चलाने के लिए समर्थन करता है । यह प्रक्रिया सामग्री है जो कंप्यूटर तंत्र का भाग है या उपलब्ध कराया गया है और जो अवधारित करता है कि उपयोजन कार्यक्रम कैसे चलते हैं । उदाहरण के लिए कोई प्रचालन आशंका ।

परीक्षण प्रमाणपत्र

आंतरिक तकनीकी परीक्षण के सीमित प्रयोजन के लिए प्रमाणीकरण प्राधिकारी द्वारा जारी अंकीय चिन्हक प्रमाणपत्र ।

आशंका

तंत्र को हानि पहुंचाने के संभावित कारण की कोई परिस्थिति या घटना जिसमें विनाश, अप्राधिकृत प्रकटन या डाटा का उपांतरण और या/सेवा का न किया जाना ।

समय समाप्त

कोई सुरक्षा विशेषता जो उपयोक्ता को सत्रांत करता है यदि विनिर्दिष्ट समय की अवधि की भीतर कोई प्रविष्टि अंतक (टर्मिनल) में नहीं की जाती है ।

समय स्टांप

ऐसा संकेतचिन्ह जो कार्य को सही तारीख और समय और व्यक्ति या युक्ति की पहचान जो समय स्टांप को उपदर्शित (कम से कम) करता है, भेजता है या प्राप्त करता है ।

संकेत

हार्डवेयर सुरक्षा संकेत में उपयोक्ता की निजी कुंजी(यां) लोक कुंजी प्रमाणपत्र और वकैल्पिकतः अन्य प्रमाणपत्र को गुप्त भेड़ार जिसके अंतर्गत उपयोक्ता की प्रमाणन श्रृंखला में सभी प्रमाणपत्र हैं, अंतर्विष्ट हो ।

संव्यवहार

कारबार सूचना का कंप्यूटर आधारित अंतरण जिसमें विश्वव्यापी नेटवर्कों पर संचार में सहायता करने के लिए विशिष्ट प्रक्रियाएं सम्मिलित हैं।

विश्वास

सामान्यतः अवधारण कि कोई निकाय वैसे ही व्यवहार करेगा जैसे उससे आशा की जाती है। विश्वास किसी विशिष्ट कृत्य को ही लागू होगा। अधिप्रमाणन नेटवर्क में इस पद भी मुख्य भूमिका अधिप्रमाणन निकाय और प्रमाणीकरण प्राधिकारी के बीच संबंध का वर्णन करना है। किसी अधिप्रमाण निकाय को इस बात का पूर्ण विश्वास होना चाहिए कि वे वैध और विश्वसनीय अंकीय चिन्हक प्रमाणपत्र तैयार करने के लिए प्रमाणीकरण प्राधिकारी पर विश्वास कर सकता है और उन अंकीय चिन्हक प्रमाणपत्रों के उपयोक्ता विश्वास को अधिप्रमाणित करने वाले निकाय के अवधारण पर विश्वास करेगा।

विश्वसनीय स्थिति

वह भूमिका जिसके अंतर्गत क्रिएटोग्राफी संक्रियाओं तकच पहुंच और उनपर नियंत्रण जो अंकीय चिन्हक प्रमाणपत्रों का निर्माण, उपयोग, निलंबन या प्रतिसंहृत को जिसके अंतर्गत ऐसी संक्रियाएं भी हैं जो किसी संग्रह तक पहुंच को निबंधित करती है तत्त्विक रूप से प्रभावित कर सके।¹³

विश्वसनीय पर व्यक्ति

साधारणतयः स्वतंत्र पक्षपातरहित पर व्यक्ति वह है जो कंप्यूटर आधारित सूचना अंतरणों की अंतिम प्रतिमूर्ति तथा विश्वसनीयता में अभिदाय करता है। विश्वसनीय पर व्यक्ति न्यासकर्ता-न्यासी या अन्य वैश्वासिक संबंध के अस्तित्व का संकेत नहीं देती है।

विश्वसनीय तंत्र

कंप्यूटर हार्डवेयर, साफ्टवेयर और प्रक्रियाएं जो युक्तियुक्त रूप से अतिक्रमण और दुरुपयोग से सुरक्षित है, उपलब्धता, विश्वसनीयता और सही संक्रिया के युक्तियुक्त स्तर का उपबंध करता है, उनके आशयित कृत्यों का पालन करने के लिए युक्तियुक्त रूप से उपयुक्त है, और लागू प्रतिमूर्ति नीति को प्रकृत करता है। विश्वसनीय पद्धति अनिवार्यतः वर्गीकृत सरकारी नाम पद्धति के यथा मान्यताप्राप्त “विश्वसनीय तंत्र” नहीं है।

प्रकार (प्रमाणपत्र का)

किसी अंकीय चिन्हक प्रमाणपत्र की परिमाणित करने वाली विशेषताएं जो इसके उपयोजनों के किसी वर्ग के आशयित प्रयोजन अनन्य रूप से सीमित करता है, उस प्रकार से सहबद्ध है।

असंदिग्ध नाम (सुमिन्न नाम देखिए)

एक समान संसधान स्थान निर्धारक (यू आर एल)

वर्ल्ड वाइड वेब पर अवस्थित कतिपय अभिलेखों और अन्य संसाधनों का अभिज्ञान करणों और पता लगाने के लिए मानकीकृत युक्ति है।

उपयोक्ता

ऐसा प्राधिकारी निकाय जो आवेदक अभिदाता, प्राप्तिकर्ता या विश्वसनीय पक्षकार के रूप में प्रमाणपत्र का उपयोग करता है, किन्तु इसके अंकीय चिन्हक प्रमाणपत्र जारी करने वाला अंकीय चिन्हक प्रमाणपत्र जारी करने वाला प्रमाणकर्ता प्राधिकारी नहीं है (प्रमाणपत्र आवेदक, निकाय, व्यक्ति, अभिदाता भी देखें)

वैध प्रमाणपत्र

इसमें सूचीबद्ध किसी प्रमाणकर्ता प्राधिकारी द्वारा जारी और अभिदाता द्वारा स्वीकार किया गया अंकीय चिन्हक प्रमाणपत्र।

किसी प्रमाणपत्र को विधिमान्य करना (अर्थात् अंतिम उपयोक्ता या अभिदाता प्रमाणपत्र का)

प्राप्तकर्ता या विश्वासनीय पक्षकार द्वारा निष्पादित प्रक्रिया यह पुष्टि करने के लिए कि अंतिम उपयोक्ता अभिदाता अंकीय चिन्हक प्रमाणपत्र विधिमान्य है उस तारीख और समय पर संप्रवर्तनीय था जब उपयुक्त अंकीय चिन्हक का सृजन किया गया था ।

विधिमान्यकरण (प्रमाणपत्र आवेदन का)

आवेदन के अनुमोदन और अंकीय चिन्हक प्रमाणपत्र के निर्गम की एक पूर्व अपेक्षा के रूप में किसी अंकीय चिन्हक प्रमाणपत्र आवेदन के प्रस्तुतिकरण के पश्चात् प्रमाणकर्ता प्राधिकारी या इसके अभिकर्ता द्वारा निष्पादित प्रक्रिया (अधिप्रमाणन, साप्टवेयर विधिमान्यकरण भी देखिए)

विधिमान्यकरण (साप्टवेयर का) (साप्टवेयर का विधिमान्यकरण देखिए)

सत्यापन करना (अंकीय चिन्हक)

व्याकरणिक रूप भेदों और सजातीय पदों के साथ किसी अंकीय चिन्हक इलैक्ट्रॉनिक अभिलेख या लोक कुंजी से यह अवधारित करना अभिप्रेत है कि क्या —

(क) आरंभिक इलैक्ट्रॉनिक अभिलेख अभिदाता की लोक कुंजी तत्संबंधी निजी कुंजी के उपयोग से अंकीय चिन्हक चिपकाए गए थे ।

(ख) आरंभिक इलैक्ट्रॉनिक अभिलेख अकिल रूप प्रतिधारित किया जाता है या उसमें परिवर्तन किया गया है क्योंकि सा इलैक्ट्रॉनिक अभिलेख अंकीय चिन्हक के ऐसे चिपकाए गए थे ।

वायरस

किसी कंप्यूटर अनुदेश, सूचना डाटा या कार्यक्रम से अभिप्रेत ऐसा वायरस है जो किसी कंप्यूटर संसाधन के निष्पादन को नष्ट करता है, नुकसान पहुंचाता है, अवश्रेणीकृत करता है या प्रतिकूल रूप से प्रभावित करता है या किसी अन्य कंप्यूटर संसाधन के साथ स्वयं को संलग्न करता है और तब प्रचालित होता जब उस कंप्यूटर संसाधन में कोई कार्यक्रम, आकड़ा या अनुदेश क्रियान्वित किया जाता है कोई अन्य घटना घटती है ।

भेद्यता

ऐसा दोष है जिसे पद्धति या उन आस्तियों जो इसमें अन्तर्विष्ट हैं, को नुकसान पहुंचाने के लिए उपयोग में लाया जा सकता है ।

वेब ब्रोसर

ऐसा साप्टवेयर उपयोजन जो वेब पृष्ठों का पता लगाने या उन्हें प्रदर्शित करने के लिए उपयोग किया जाता है ।

वर्ल्ड वाइड वेब (डब्ल्यू डब्ल्यू डब्ल्यू)

हाइपरटेक्स्ट आधारित वितरित सूचना पद्धति वह पद्धति है जिसमें उपयोक्त हाइपरटेक्स्ट दस्तावेजों को सृजित संपादित कर सकेगा या उन्हें देख सकेगा । आलेखी दस्तावेज का प्रकाशन और माध्यम का पुनः प्राप्ति, संबद्ध दस्तावेजों का संग्रहण जो इंटरनेट पर उपस्थित हैं ।

लेखन

अभिलेखन की वह सूचना जो पश्चात् वर्ती निर्देश के संबंध में गम्य और प्रयोज्य है ।

एक्स 509

अंकीय चिन्हक प्रमाणपत्रों के लिए आई टी यू टी (अन्तरराष्ट्रीय दूर संचार संघ ही) मानक । एक्स 509 वी3 उन प्रमाणपत्रों को निर्दिष्ट करता है जिनके विस्तारण अन्तर्विष्ट हैं या उन्हें अन्तर्विष्ट करने की क्षमता है ।

एक्सोनिम्स

प्रा.प्र.सू.

प्राधिकार प्रतिसंहरण सूची

प्र.प्रा	प्रमाणन प्राधिकारी
प्र.नी.	प्रमाणपत्र नीति
प्र.व्य.क.	प्रमाणन व्यवहार कथन
प्र.प्र.सू.	प्रमाणपत्र प्रतिसंहरण सूची
प्र.चि.अ.	प्रमाणपत्र चिह्नक अनुरोध
सु.ना.	सुमिन्न नाम
ई.मेल	इलैक्ट्रॉनिक मेल
फा.अ.न्या.	फाइल अंतरण न्याचार
एकी.से.अ.ने.	एकीकृत सेवा अंकीय नेटवर्क
अ.दूर.सं.	अंतरराष्ट्रीय दूरसंचार संघ
स्था.क्षे.नेट.	स्थानीय क्षेत्र नेटवर्क
पिन	व्यक्तिगत पहचान संख्या
लो.कुं.अ.	लोक कुंजी अवसंरचना
लो.कुं.अ. x .509	लोक कुंजी अवसंरचना x .509
स.सं.स्था.नि.	समान संसाधान स्थान निर्धारक
वि.क्षे.नेट.	विस्तृत क्षेत्र नेटवर्क

[सं. 1(20)/97-II डी (एन II)/एफ 6(ii)]

पी. एम. सिंह, संयुक्त सचिव

NOTIFICATION

New Delhi, the 17th October, 2000

G.S.R. 789(E).—In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the application and other guidelines for Certifying Authorities, namely:—

1. Short title and commencement.—(1) These Rules may be called Information Technology (Certifying Authorities) Rules, 2000.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.—In these Rules, unless the context otherwise requires,—

(a) “Act” means the Information Technology Act, 2000 (21 of 2000);

(b) “applicant” means Certifying Authority applicant;

(c) “auditor” means any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority;

(d) “Controller” means Controller of Certifying Authorities appointed under sub-section (1) of Section 17 of the Act;

(e) "Digital Signature Certificate" means Digital Signature Certificate issued under sub-section (4) of section 35 of the Act;

(f) "information asset" means all information resources utilized in the course of any organisation's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks);

(g) "licence" means a licence granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;

(h) "licensed Certifying Authority" means Certifying Authority who has been granted a licence to issue Digital Signature Certificates;

(i) "person" shall include an individual; or a company or association or body of individuals; whether incorporated or not; or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments;

(j) "Schedule" means a schedule annexed to these rules;

(k) "subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

(l) "trusted person" means any person who has: –

- (i) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority; or
- (ii) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities.

(m) words and expressions used herein and not defined but defined in Schedule-IV shall have the meaning respectively assigned to them in that schedule.

3. The manner in which information be authenticated by means of Digital Signature.- A Digital Signature shall,-

- (a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again;

(b) use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

Explanation: Computer equipment and software utilizing two such keys are often termed as "asymmetric cryptography".

4. Creation of Digital Signature.- To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; and the Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record.

5. Verification of Digital Signature.- The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifier shall check-

(i) if the Digital Signature was created using the corresponding private key; and

(ii) if the newly computed hash result matches the original result which was transformed into Digital Signature during the signing process. The verification software will confirm the Digital Signature as verified if:-

(a) the signer's private key was used to digitally sign the electronic record, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and

(b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

6. Standards.-The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority's functions are as under:

The product	The standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509, version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	DSA and RSA
Digital Hash Function	MD5 and SHA-1
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a user's private keys and certificates
Distinguished name	X.520
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10

7. Digital Signature Certificate Standard.- All Digital Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 standard as per rule 6 and shall *inter alia* contain the following data, namely:-

- (a) Serial Number (assigning of serial number to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate);
- (b) Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate);
- (c) Issuer Name (name of the Certifying Authority who issued the Digital Signature Certificate);
- (d) Validity period of the Digital Signature Certificate;
- (e) Name of the subscriber (whose public key the Certificate identifies); and
- (f) Public Key information of the subscriber.

8. Licensing of Certifying Authorities.— (1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely :-

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;

(b) a company having –

(i) paid up capital of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being the Hindu Undivided Family, firm or company:

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company:

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company-

(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(c) a firm having –

(i) capital subscribed by all partners of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners:

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national:

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm-

- (i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;
- (ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.- For the purpose of this rule,-

(i) “company” shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act, 1961 (43 of 1961);

(ii) “firm”, “partner” and “partnership” shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression “partner” shall also include any person who, being a minor has been admitted to the benefits of partnership;

(iii) “foreign company” shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act, 1961 (43 of 1961);

(iv) "net worth" shall have the meaning assigned to it in clause (ga) of sub-section (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

(v) "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act, 1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall submit a performance bond or furnish a banker's guarantee from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than five crores of rupees and the performance bond or banker's guarantee shall remain valid for a period of six years from the date of its submission:

Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of sub-rule (1) shall submit a performance bond or furnish a banker's guarantee for ten crores of rupees:

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the performance bond or banker's guarantee may be invoked –

- (a) when the Controller has suspended the licence under sub-section (2) of section 25 of the Act; or
- (b) for payment of an offer of compensation made by the Controller; or
- (c) for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or
- (d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's licence or operations is discontinued; or
- (e) any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation.— "transfer of operation" shall have the meaning assigned to it in clause (47) of section 2 of the Income-tax Act, 1961 (43 of 1961).

9. Location of the Facilities.—The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.

10. Submission of Application.— Every application for a licensed Certifying Authority shall be made to the Controller,—

- (i) in the form given at Schedule-I; and
- (ii) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall *inter alia* include—
 - (a) a Certification Practice Statement (CPS);
 - (b) a statement including the procedures with respect to identification of the applicant;
 - (c) a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;
 - (d) certified copies of the business registration documents of Certifying Authority that intends to be licensed;
 - (e) a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;
 - (f) an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;
 - (g) an undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;
 - (h) an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2) of rule 8 within one month of

Controller indicating his approval for the grant of licence to operate as a Certifying Authority;

- (i) any other information required by the Controller.

11. Fee.— (1) The application for the grant of a licence shall be accompanied by a non-refundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority's licence shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

12. Cross Certification.— (1) The licensed Certifying Authority shall have arrangement for cross certification with other licensed Certifying Authorities within India which shall be submitted to the Controller before the commencement of their operations as per rule 20:

Provided that any dispute arising as a result of any such arrangement between the Certifying Authorities; or between Certifying Authorities or Certifying Authority and the Subscriber, shall be referred to the Controller for arbitration or resolution.

(2) The arrangement for Cross Certification by the licensed Certifying Authority with a Foreign Certifying Authority along with the application, shall be submitted to the Controller in such form and in such manner as may be provided in the regulations made by the Controller; and the licensed Certifying Authority shall not commence cross certification operations unless it has obtained the written or digital signature approval from the Controller.

13. Validity of licence.— (1) A licence shall be valid for a period of five years from the date of its issue.

(2) The licence shall not be transferable.

14. Suspension of Licence.— (1) The Controller may by order suspend the licence in accordance with the provisions contained in sub-section (2) of section 25 of the Act.

(2) The licence granted to the persons referred to in clauses (a) to (c) of sub-rule (1) of rule 8 shall stand suspended when the performance bond submitted or the banker's guarantee furnished by such persons is invoked under sub-rule (2) of that rule.

15. Renewal of licence.— (1) The provisions of rule 8 to rule 13, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed Certifying Authority.

(2) A Certifying Authority shall submit an application for the renewal of its licence not less than forty-five days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

16. Issuance of Licence.— (1) The Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he may deem fit, grant or renew the licence or reject the application:

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed Certifying Authority is approved, the applicant shall—

(a) submit a performance bond or furnish a banker's guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 8; and

(b) execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the rules made thereunder.

17. Refusal of Licence.- The Controller may refuse to grant or renew a licence if-

- (i) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or
- (ii) the applicant is in the course of being wound up or liquidated; or
- (iii) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or
- (iv) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or
- (v) the Controller has invoked performance bond or banker's guarantee; or
- (vi) a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or
- (vii) a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or
- (viii) the audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or
- (ix) a Certifying Authority fails to comply with the directions of the Controller.

18. Governing Laws.- The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

19. Security Guidelines for Certifying Authorities.- (1) The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering

classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule-II and Schedule-III respectively.

(3) The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation:

Provided that any change made by the Certifying Authority in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

20. Commencement of Operation by Licensed Certifying Authorities.— The licensed Certifying Authority shall commence its commercial operation of generation and issue of Digital Signature only after -

- (a) it has confirmed to the Controller the adoption of Certification Practice Statement;
- (b) it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller;
- (c) the installed facilities and infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 31; and
- (d) it has submitted the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

21. Requirements Prior to Cessation as Certifying Authority.— Before ceasing to act as a Certifying Authority, a Certifying Authority shall, -

- (a) give notice to the Controller of its intention to cease acting as a Certifying Authority;

Provided that the notice shall be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence.

(b) advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;

(c) notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Signature Certificate issued by it :

Provided that the notice shall be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Signature Certificate, as the case may be;

(d) the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;

(e) revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;

(f) make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates;

(g) make reasonable arrangements for preserving the records for a period of seven years;

(h) pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry;

(i) after the date of expiry mentioned in the licence, the Certifying Authority shall destroy the certificate—signing private key and confirm the date and time of destruction of the private key to the Controller.

22. Database of Certifying Authorities.— The Controller shall maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing *inter alia* the following details:

- (a) the name of the person/names of the Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;
- (b) the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital Signature Certificate;
- (c) current and past versions of Certification Practice Statement of Certifying Authority;
- (d) time stamps indicating the date and time of -
 - (i) grant of licence;
 - (ii) confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority;
 - (iii) commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority;
 - (iv) revocation or suspension of licence of Certifying Authority;
 - (v) commencement of operation of Cross Certifying Authority;
 - (vi) issue of recognition of foreign Certifying Authority;
 - (vii) revocation or suspension of recognition of foreign Certifying Authority.

23. Digital Signature Certificate.- The Certifying Authority shall, for issuing the Digital Signature Certificates, while complying with the provisions of section 35 of the Act, also comply with the following, namely:-

- (a) the Digital Signature Certificate shall be issued only after a Digital Signature Certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it:

Provided that the application Form contains, *inter alia*, the particulars given in the modal Form given in Schedule-IV;

- (b) no interim Digital Signature Certificate shall be issued;

(c) the Digital Signature Certificate shall be generated by the Certifying Authority upon receipt of an authorised and validated request for:-

- (i) new Digital Signature Certificates;
- (ii) Digital Signature Certificates renewal;

(d) the Digital Signature Certificate must contain or incorporate, by reference such information, as is sufficient to locate or identify one or more repositories in which revocation or suspension of the Digital Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked;

(e) the subscriber identity verification method employed for issuance of Digital Signature Certificate shall be specified in the Certification Practice Statement and shall be subject to the approval of the Controller during the application for a licence;

(f) where the Digital Signature Certificate is issued to a person (referred to in this clause as a New Digital Signature Certificate) on the basis of another valid Digital Signature Certificate held by the said person (referred in this clause as an Originating Digital Signature Certificate) and subsequently the originating Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new Digital Signature Certificate;

(g) the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted;

(h) if the subscriber accepts the issued Digital Signature Certificate, the Certifying Authority shall publish a signed copy of the Digital Signature Certificate in a repository;

(i) where the Digital Signature Certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact, or otherwise, that affects the validity or reliability of such Digital Signature Certificate, it shall notify the same to the subscriber immediately;

(j) all Digital Signature Certificates shall be issued with a designated expiry date.

24. Generation of Digital Signature Certificate.— The generation of the Digital Signature Certificate shall involve:

- (a) receipt of an approved and verified Digital Signature Certificate request;
- (b) creating a new Digital Signature Certificate;
- (c) binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner;
- (d) issuing the Digital Signature Certificate and the associated public key for operational use;
- (e) a distinguished name associated with the Digital Signature Certificate owner; and
- (f) a recognized and relevant policy as defined in Certification Practice Statement.

25. Issue of Digital Signature Certificate.— Before the issue of the Digital Signature Certificate, the Certifying Authority shall:—

- (i) confirm that the user's name does not appear in its list of compromised users;
- (ii) comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;
- (iii) comply with all privacy requirements;
- (iv) obtain a consent of the person requesting the Digital Signature Certificate, that the details of such Digital Signature Certificate can be published on a directory service.

26. Certificate Lifetime.— (1) A Digital Signature Certificate,—

- (a) shall be issued with a designated expiry date;
- (b) which is suspended shall return to the operational use, if the suspension is withdrawn in accordance with the provisions of section 37 of the Act;
- (c) shall expire automatically upon reaching the designated expiry date at which time the Digital Signature Certificate shall be archived;
- (d) on expiry, shall not be re-used.

(2) The period for which a Digital Signature Certificate has been issued shall not be extended, but a new Digital Signature Certificate may be issued after the expiry of such period.

27. Archival of Digital Signature Certificate.- A Certifying Authority shall archive -

- (a) applications for issue of Digital Signature Certificates;
- (b) registration and verification documents of generated Digital Signature Certificates;
- (c) Digital Signature Certificates;
- (d) notices of suspension;
- (e) information of suspended Digital Signature Certificates;
- (f) information of revoked Digital Signature Certificates;
- (g) expired Digital Signature Certificates,

for a minimum period of seven years or for a period in accordance with legal requirement.

28. Compromise of Digital Signature Certificate.- Digital Signature Certificates in operational use that become compromised shall be revoked in accordance with the procedure defined in the Certification Practice Statement of Certifying Authority

Explanation : Digital Signature Certificates shall,-

- (a) be deemed to be compromised where the integrity of:-
 - (i) the private key associated with the Digital Signature Certificate is in doubt;
 - (ii) the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes;
- (b) remain in the compromised state for only such time as it takes to arrange for revocation.

29. Revocation of Digital Signature Certificate.- (1) Digital Signature Certificate shall be revoked and become invalid for any trusted use, where -

- (a) there is a compromise of the Digital Signature Certificate owner's private key;
- (b) there is a misuse of the Digital Signature Certificate;

- (c) there is a misrepresentation or errors in the Digital Signature Certificate;
- (d) the Digital Signature Certificate is no longer required.

(2) The revoked Digital Signature Certificate shall be added to the Certificate Revocation List (CRL).

30. Fees for issue of Digital Signature Certificate.—(1) The Certifying Authority shall charge such fee for the issue of Digital Signature Certificate as may be prescribed by the Central Government under sub-section (2) of section 35 of the Act.

(2) Fee may be payable in respect of access to Certifying Authority's X.500 directory for certificate downloading. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.

(3) Fees may be payable in respect of access to Certifying Authority's X.500 directory service for certificate revocation or status information. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing the fee schedule on a nominated website.

(4) No fee is to be levied for access to Certification Practice Statement via Internet. A fee may be charged by the Certifying Authority for providing printed copies of its Certification Practice Statement.

31. Audit.—(1) The Certifying Authority shall get its operations audited annually by an auditor and such audit shall include *inter alia*,

- (i) security policy and planning;
- (ii) physical security;
- (iii) technology evaluation;
- (iv) Certifying Authority's services administration;
- (v) relevant Certification Practice Statement;
- (vi) compliance to relevant Certification Practice Statement;
- (vii) contracts/agreements;
- (viii) regulations prescribed by the Controller;
- (ix) policy requirements of Certifying Authorities Rules, 2000.

(2) The Certifying Authority shall conduct,-

- (a) half yearly audit of the Security Policy, physical security and planning of its operation;
- (b) a quarterly audit of its repository.

(3) The Certifying Authority shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities.

32. Auditor's relationship with Certifying Authority.- (1) The auditor shall be independent of the Certifying Authority being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.

(2) The auditor and the Certifying Authority shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

33. Confidential Information.- The following information shall be confidential namely:--

- (a) Digital Signature Certificate application, whether approved or rejected;
- (b) Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital Signature Certificate information;
- (c) subscriber agreement.

34. Access to Confidential Information.- (1) Access to confidential information by Certifying Authority's operational staff shall be on a "need-to-know" and "need-to-use" basis.

(2) Paper based records, documentation and backup data containing all confidential information as prescribed in rule 33 shall be kept in secure and locked container or filing system, separately from all other records.

(3) The confidential information shall not be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

SCHEDULE-I

[See rule 10]

Form for Application for grant of Licence to be a Certifying Authority**For Individual**

1. Full Name *

Last Name/Surname _____

First Name _____

Middle Name _____

2. Have you ever been known by any other name? If Yes,

Last Name/Surname _____

First Name _____

Middle Name _____

3. Address

A. Residential Address *

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

State/Union Territory _____ Pin : _____

Telephone No. _____

Fax _____

Mobile Phone No. _____

B. Office Address *

Name of Office _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

State/Union Territory _____ Pin : _____

Telephone No. _____

Fax _____

4. Address for Communication * Tick √ as applicable A or B

5. Father's Name *

Last Name/Surname _____

First Name _____

Middle Name _____

6. Sex * (For Individual Applicant only) Tick √ as applicable : Male / Female

7. Date of Birth (dd/mm/yyyy) * ---/---/----

8. Nationality *

9. Credit Card Details

Credit Card Type _____

Credit Card No. _____

Issued By _____

10. E-mail Address _____

11. Web URL address _____

12. Passport Details #

Passport No. _____

Passport issuing authority _____

Passport expiry date (dd/mm/yyyy) ---/---/----

13. Voter's Identity Card No. # _____

14. Income Tax PAN no. # _____

15. ISP Details

ISP Name * _____

ISP's Website Address, if any _____

Your User Name at ISP, if any _____

16. Personal Web page URL address, if any _____

17. Capital in the business or profession * Rs. _____

(Attach documentary proof)

For Company /Firm/Body of Individuals/Association of Persons/ Local Authority

18. Registration Number * _____

19. Date of Incorporation/Agreement/Partnership * ---/---/---

20. Particulars of Business, if any: *

Head Office _____

Name of Office _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____ Pin _____

State/Union Territory _____

Telephone No. _____

Fax _____

Web page URL address, if any _____

No. of Branches _____

Nature of Business _____

21. Income Tax PAN No.* _____

22. Turnover in the last financial year Rs. _____

23. Net worth * Rs. _____

(Attach documentary proof)

24. Paid up Capital * Rs. _____

(Attach documentary proof)

25. Insurance Details

Insurance Policy No.* _____

Insurer Company * _____

26. Names, Addresses etc. of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given in the next page) *

No. of Partners/Members/Directors _____

Details of Partners/Members/Directors

A. Full Name

Last Name/Surname _____

First Name _____

Middle Name _____

B. Address

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

State/Union Territory Pin _____

Telephone No. _____

Fax No. _____

Mobile Phone No. _____

C. Nationality _____

In case of foreign national, Visa details _____

D. Passport Details #

Passport No. _____

Passport issuing authority _____

Passport expiry date _____

E. Voter's Identity Card No. #

F. Income Tax PAN no. #

G. E-mail Address

H. Personal Web page URL, if any

27. Authorised Representative *

Name _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

Pin _____

State/Union Territory _____
 Telephone No. _____
 Fax _____
 Nature of Business _____

For Government Ministry/Department/Agency/Authority

28. Particulars of Organisation: *

Name of Organisation _____
 Administrative Ministry/Department _____
 Under State/Central Government _____
 Flat/Door/Block No. _____
 Name of Premises/Building/Village _____
 Road/Street/Lane/Post Office _____
 Area/Locality/Taluka/Sub-Division _____
 Town/City/District _____ Pin _____
 State/Union Territory _____
 Telephone No. _____
 Fax No. _____
 Web page URL Address _____
 Name of the Head of Organisation _____
 Designation _____
 E-mail Address _____

29. Bank Details

Bank Name * _____
 Branch * _____
 Bank Account No. * _____
 Type of Bank Account * _____

30. Whether bank draft/pay order for licence fee enclosed * : Y / N If yes,

Name of Bank _____
 Draft/pay order No. _____
 Date of Issue _____
 Amount _____

31. Location of facility in India for generation of Digital Signature Certificate * _____

32. Public Key [®] _____

33. Whether undertaking for Bank Guarantee/Performance Bond attached * : Y / N

(Not applicable if the applicant is a Government Ministry/Department/Agency/ Authority)

34. Whether Certification Practice Statement is enclosed * : Y / N

35. Whether certified copies of business registration document are enclosed : Y / N
(For Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority)

If yes, the documents attached:

- ✓ ii)
- iii)
- iv)

36 Any other information _____

Date

Signature of the Applicant

Instructions

- 1. Columns marked with * are mandatory.
- 2. For the columns marked with #, details for at least one is mandatory
- 3. Column No. 1 to 17 are to be filled up by individual applicant.
- 4. Column No. 18 to 27 are to be filled up if applicant is a Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority.
- 5. Column No. 28 is to be filled up if applicant is a Government organisation
- 6. Column No. 29, 30, 31 and 34 are to be filled up by all applicants
- 7. [®] Column No. 32 is applicable only for application for renewal of licence
- 8. Column No. 33 is not applicable if the applicant is a Government organisation

SCHEDULE-II

[See rule 19(2)]

Information Technology (IT) Security Guidelines**Index**

	Page
1. Introduction	27
2. Implementation of an Information Security Programme	27
3. Information Classification	28
4. Physical and Operational Security	30
4.1 Site Design.....	30
4.2 Fire Protection.....	31
4.3 Environmental Protection.....	31
4.4 Physical Access.....	32
5. Information Management	33
5.1 System Administration	33
5.2 Sensitive Information Control.	34
5.3 Sensitive Information Security.....	35
5.4 Third Party Access.....	35
5.5 Prevention of Computer Misuse.....	36
6. System integrity and security measures	36
6.1 Use of Security Systems or Facilities.....	36
6.2 System Access Control	37
6.3 Password Management...	38
6.4 Privileged User's Management.	39
6.5 User's Account Management.....	39
6.6 Data and Resource Protection.	40
7. Sensitive Systems Protection	41
8. Data Centre Operations Security	41
8.1 Job Scheduling.....	41
8.2 System Operations Procedure.	41
8.3 Media Management	42
8.4 Media Movement.....	42
9. Data Backup and Off-site Retention	43
10. Audit Trails and Verification	44
11. Measures to Handle Computer Virus	45
12. Relocation of Hardware and Software	46
13. Hardware and Software Maintenance	46
14. Purchase and Licensing of Hardware and Software	47
15. System Software	48
16. Documentation Security	49
17. Network Communication Security	49
18. Firewalls	50
19. Connectivity	51
20. Network Administrator	51
21. Change Management	52
21.1 Change Control.....	52
21.2 Testing of Changes to Production System.....	52
21.3 Review of Changes.....	53
22. Problem Management and Reporting	53
23. Emergency Preparedness	53
24. Contingency Recovery Equipment and Services	54
25. Security Incident Reporting and Response	54
26. Disaster Recovery/Management	54

Information Technology (IT) Security Guidelines

1. Introduction

This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organizations to develop internal processes that meet the guidelines set forth in this document.

The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

- shall: The guideline defined is a mandatory requirement, and therefore must be complied with.
- should: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- must: The guideline defined is a mandatory requirement, and therefore must be complied with.
- may: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows:

- (a) Adoption of a security policy;
- (b) Security risk analysis;
- (c) Development and implementation of a information classification system;
- (d) Development and implementation of the security standards manual;
- (e) Implementation of the management security self-assessment process;
- (f) On-going security programme maintenance and enforcement; and
- (g) Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established.

When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access. It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organization, it is necessary to advise them on which types

of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorized disclosure/use could cause serious damage to the organization, e.g. strategic planning documents.

Restricted is that classification of information of which unauthorized disclosure/use would not be in the best interest of the organization and/or its customers, e.g. design details, computer software (programs, utilities), documentation, organization personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, e.g. operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure e.g. published annual reports, periodicals.

While the above classifications are appropriate for a general organization view point, the following classifications may be considered :

Top Secret: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Design

- (1) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.
- (2) As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.
- (3) Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.
- (4) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.
- (5) External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.
- (6) Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.
- (7) Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other

agencies of the Central or State Government shall be installed at the operational site.

- (8) Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.
- (9) Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/ disaster recovery plan.

4.2 Fire Protection

- (1) Combustible materials shall not be stored within hundred meters of the operational site.
- (2) Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.
- (3) Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.
- (4) Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.
- (5) Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.
- (6) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection

- (1) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.
- (2) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

- (3) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.
- (4) Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access

- (1) Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.
- (2) Biometric physical access security systems shall be installed to control and audit access to the operational site.
- (3) Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.
- (4) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.
- (5) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.
- (6) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.
- (7) Emergency exits shall be tested periodically to ensure that the access security systems are operational.
- (8) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 System Administration

- (1) Each organization shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.
- (2) Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.
- (3) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.
- (4) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.
- (5) Periodic review of the access rights of all users must be performed.
- (6) The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).
- (7) The System Administrator must take steps to safeguards classified information as prescribed by its owner.
- (8) The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.

- (9) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.
- (10) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.
- (11) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.
- (12) The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.
- (13) The System Administrator should ensure that no generic user is enabled or active on the system.

5.2 Sensitive Information Control

- (1) Information assets shall be classified and protected according to their sensitivity and criticality to the organization.
- (2) Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.
- (3) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.
- (4) All sensitive material shall be stamped or labeled accordingly.
- (5) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.
- (6) Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.
- (7) Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive,

tapes etc.) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 Sensitive Information Security

- (1) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.
- (2) Highly sensitive information shall be classified in accordance with para 3.
- (3) Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.
- (4) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.
- (5) Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.
- (6) Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 Third Party Access

- (1) Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.
- (2) In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.
- (3) The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5 Prevention of Computer Misuse

- (1) Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.
- (2) Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.
- (3) Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include :
 - (i) Prompt reporting of suspected breach;
 - (ii) Proper investigation and assessment of the nature of suspected breach;
 - (iii) Secure evidence and preserve integrity of such material as relates to the discovery of any breach;
 - (iv) Remedial measures.
- (4) All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
- (5) Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:
 - (i) The role of the System Administrator, System Security Administrator and management;
 - (ii) Procedure for investigation;
 - (iii) Areas for security review; and
 - (iv) Subsequent follow-up action.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

- (1) Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining

entry to the information system and to prevent unauthorised access to data.

(2) Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 System Access Control

- (1) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.
- (2) Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.
- (3) The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "gæ .e" etc. to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.
- (4) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorisations shall be developed, documented and implemented.
- (5) An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.
- (6) Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.
- (7) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.
- (8) Stored passwords shall be protected by access controls from unauthorised disclosure and modification.

- (9) Automatic time-out for terminal inactivity should be implemented.
- (10) Audit trail of security-sensitive access and actions taken shall be logged.
- (11) All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.
- (12) Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.
- (13) Activities of all remote users shall be logged and monitored closely.
- (14) The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.
- (15) The startup and shutdown procedure of the security software must be automated.
- (16) Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 Password Management

- (1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:
 - (i) Minimum of eight characters without leading or trailing blanks;
 - (ii) Shall be different from the existing password and the two previous ones;
 - (iii) Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and
 - (iv) Shall not be shared, displayed or printed.

- (2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.
- (3) Passwords which are easy-to-guess (e.g. user name, birth date, month, standard words etc.) should be avoided.
- (4) Initial or reset passwords must be changed by the user upon first use.
- (5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.
- (6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 Privileged User's Management

- (1) System privileges shall be granted to users only on a need-to-use basis.
- (2) Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.
- (3) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.
- (4) Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.
- (5) Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.
- (6) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 User's Account Management

- (1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:
 - (i) Users shall be authorised by the computer system owner to access the computer services.
 - (ii) A written statement of access rights shall be given to all users.

- (iii) All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.
- (iv) Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgement of receipt of the accounts by the users.
- (v) A formal record of all registered users of the computer services shall be maintained.
- (vi) Access rights of users who have been transferred, or left the organisation shall be removed immediately.
- (vii) A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.
- (viii) Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

- (i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.
- (ii) immediately upon the termination of the services of an individual.
- (iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 Data and Resource Protection

(1) All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.

(2) The operating system or security system of the computer system shall:

- (i) Define user authority and enforce access control to data within the computer system;

(ii) Be capable of specifying, for each named individual, a list of named data objects (e.g. file, programme) or groups of named objects, and the type of access allowed.

(3) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

(4) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

(5) Application Programmer shall not be allowed to access the production system.

7. **Sensitive Systems Protection**

(1) Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system.

(2) For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.

(3) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. **Data Centre Operations Security**

8.1 **Job Scheduling**

(1) Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.

(2) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 **System Operations Procedure**

(1) Procedures shall be established to ensure that only authorised and correct job stream and parameter changes are made.

(2) Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.

(3) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.

(4) Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management

- (1) Responsibilities for media library management and protection shall be clearly defined and assigned.
- (2) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.
- (3) Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorised to enter the library shall be maintained.
- (4) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.
- (5) A media management system shall be in place to account for all media stored on-site and off-site.
- (6) All incoming/outgoing media transfers shall be authorised by management and users.
- (7) An independent physical inventory check of all media shall be conducted at least every six months.
- (8) All media shall have external volume identification. Internal labels shall be fixed, where available.
- (9) Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.
- (10) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 Media Movement

- (1) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.
- (2) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.
- (3) Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

- (1) Back-up procedures shall be documented, scheduled and monitored.
- (2) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:
 - (i) Data files
 - (ii) Utilities programmes
 - (iii) Databases
 - (iv) Operating system software
 - (v) Applications system software
 - (vi) Encryption keys
 - (vii) Pre-printed forms
 - (viii) Documentation (including a copy of the business continuity plans)
- (3) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
- (4) Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.
- (5) Data backup is required for all systems including personal computers, servers and distributed systems and databases.

- (6) Critical system data and file server software must have full backups taken weekly.
- (7) The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.
- (8) Critical system data and file server software must have incremental backups taken daily.
- (9) Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.
- (10) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.
- (11) The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trails and Verification

- (1) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.
- (2) Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:
 - (i) Success or failure of the event
 - (ii) Use of authentication keys, where applicable
- (3) Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:

- (i) Significant computer system events (e.g. configuration updates, system crashes)
- (ii) Security profile changes
- (iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators
- (4) The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.
- (5) The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.
- (6) Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.
- (7) Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus

- (1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.
- (2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.
- (3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.
- (4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of

anti-virus software is loaded on all data, file, PKI servers and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures inter alia shall include:

- (i) Communication to other business partners and users who may be at risk from an infected resource
- (ii) Eradication and recovery procedures
- (iii) Incident report must be documented and communicated per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply:

- (i) All removable media will be removed from the computer system and kept at secure location.
- (ii) Internal drives will be overwritten, reformatted or removed as the situation may be.
- (iii) If applicable, ribbons will be removed from printers.
- (iv) All paper will be removed from printers.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

- (1) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.
- (2) Maintenance of an inventory and configuration chart of hardware.
- (3) Identification and use of security features implemented within hardware.
- (4) Authorization, documentation, and control of change made to the hardware.
- (5) Identification of support facilities including power and air conditioning.

- (6) Provision of an uninterruptible power supply.
- (7) Maintenance of equipment and services.
- (8) Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.
- (9) Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.
- (10) Maintenance personnel will sign non-disclosure agreements.
- (11) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.
- (12) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorized personnel of the organisation.
- (13) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.
- (14) If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

- (1) Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.
- (2) Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in

place to ensure that the implementation and operation of that software does not compromise the security of the system.

- (3) There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.
- (4) It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.
- (5) No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.
- (6) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software

- (1) All system software options and parameters shall be reviewed and approved by the management.
- (2) System software shall be comprehensively tested and its security functionality validated prior to implementation.
- (3) All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.
- (4) Versions of system software installed on the computer system and communication devices shall be regularly updated.
- (5) All changes proposed in the system software must be appropriately justified and approved by an authorised party.
- (6) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.
- (7) Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".

- (8) There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.
- (9) System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.
- (10) Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. **Documentation Security**

- (1) All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.
- (2) All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.
- (3) Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.
- (4) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.
- (5) Documentation shall be classified according to the sensitivity of its contents/implications.
- (6) Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security

- (1) All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.
- (2) The network configuration and inventories shall be documented and maintained.
- (3) Prior authorization of the Network Administrator shall be obtained for making any changes to the network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.
- (4) Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to "Physical Access".
- (5) Communication and network systems shall be controlled and restricted to authorized individuals only in accordance with para 6.2 – System Access Control.
- (6) As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.
- (7) Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls

- (1) Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.
- (2) Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.

- (3) All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.
- (4) All web servers for access by Internet users shall be isolated from other data and host servers.

19. Connectivity

- (1) Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.
- (2) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.
- (3) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.
- (4) As far as possible, no Internet access should be allowed to database server/ file server or server hosting sensitive data.
- (5) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

- (1) Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.
- (2) Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.
- (3) System must include a mechanism for alerting the Network Administrator

of possible breaches in security, e.g., unauthorized access, virus infection and hacking.

- (4) Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.
- (5) Only authorized and legal software shall be used on the network.
- (6) Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 – System Integrity and Security Measures.

21. Change Management

21.1 Change Control

- (1) Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.
- (2) A risk and impact analysis, classification and prioritisation process shall be established.
- (3) No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.
- (4) Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.
- (5) Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.
- (6) Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.
- (7) Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing Of Changes To Production System

- (1) All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.
- (2) All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.

21.3 Review Of Changes

- (1) Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.
- (2) Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.
- (3) All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.
- (4) Periodic management reports on the status of the changes implemented in the computer resource in the production system shall be submitted for management review.

22. Problem Management and Reporting

- (1) Procedures for identifying, reporting and resolving problems, such as non-functioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.
- (2) A help desk shall be set up to assist users in the resolution of problems.
- (3) A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources.

23. Emergency Preparedness

- (1) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.
- (2) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

- (1) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.
- (2) The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.
- (3) The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response

- (1) All security related incidents must be reported to a central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.
- (2) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.
- (3) Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

- (1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

- (a) emergency procedures, describing the immediate action to be taken in case of a major incident
- (b) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site
- (c) restoration procedures, describing the action to be taken to return to normal operation at the original site

(2) The documentation should include:

- (a) definition of a disaster;
- (b) condition for activating the plan;
- (c) stages of a crisis;
- (d) who will make decisions in the crisis;
- (e) role of individuals for each component of the plan;
- (f) composition of the recovery team; and
- (g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

SCHEDULE-III

[See rule 19(2)]

Security Guidelines for Certifying Authorities**Index**

	Page
1. Introduction	57
2. Security Management.....	57
3. Physical controls – site location, construction and physical access	57
4. Media Storage.....	60
5. Waste Disposal.....	60
6. Off-site Backup.....	60
7. Change and Configuration Management.....	60
8. Network and Communications Security.....	61
9. System Security Audit Procedures.....	61
9.1 Types of event recorded.....	61
9.2 Frequency of Audit Log Monitoring.....	63
9.3 Retention Period for Audit Log.....	63
9.4 Protection of Audit Log.....	63
9.5 Audit Log Backup Procedures.....	64
9.6 Vulnerability Assessments.....	64
10. Records Archival.....	64
11. Compromise and Disaster Recovery.....	65
11.1 Computing Resources, Software and/or Data are Corrupted.....	65
11.2 Secure facility after a natural or other type of disaster.....	65
11.3 Incident Management Plan.....	65
12. Number of Persons required per task.....	66
13. Identification and Authentication for each role.....	66
14. Personnel Security Controls.....	67
15. Training Requirements.....	67
16. Retaining Frequency and Requirements	67
17. Documentation supplied to Personnel.....	68
18. Key Management.....	68
18.1 Generation.....	68
18.2 Distribution of keys.....	68
18.3 Storage.....	68
18.4 Usage.....	68
18.5 Certifying Authority's Public Key Delivery to Users.....	69
19. Private Key Protection and Backup.....	69
20. Method of Destroying Private Key.....	69
21. Usage Periods for the Public and Private Keys.....	69
21.1 Key Change.....	69
21.2 Destruction	70
21.3 Key Compromise.....	70
22. Confidentiality of Subscriber's Information.....	70

Security Guidelines for Certifying Authorities

1. Introduction

This document prescribes security guidelines for the management and operation of Certifying Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certifying Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

- (1) Verification of registration, suspension and revocation request;
- (2) Generation, issuance, suspension and revocation of Digital Signature Certificates; and
- (3) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management

The Certifying Authority shall define Information Technology security policies for its operation on the lines defined in Schedule-II and Schedule-III. The policy shall be communicated to all personnel and widely published throughout the organisation to ensure that the personnel follow the policies.

3. Physical controls – site location, construction and physical access

- (1) The site location, design, construction and physical security of the operational site of Certifying Authority shall be in accordance with para 4 of the Information Technology Security Guidelines given at Schedule-II.
- (2) Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorized individuals only in accordance with para 4.4 of the Information Technology Security Guidelines given at Schedule-II.

(3) A Certifying Authority must:

- (i) ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.2 of the Information Technology Security Guidelines given at Schedule-II.
- (ii) ensure that power and air-conditioning facilities are installed in accordance with para 4.1 of the Information Technology Security Guidelines given at Schedule-II.
- (iii) ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.
- (iv) ensure unescorted access to Certifying Authority's server is limited to those personnel identified on an access list.
- (v) ensure that the exact location of Digital Signature Certification System shall not be publicly identified.
- (vi) ensure that access security system is installed to control and audit access to the Digital Signature Certification System.
- (vii) ensure that dual control over the inventory and access cards/keys are in place.
- (viii) ensure that up-to-date list of personnel who possess the access cards/keys is maintained at the Certifying Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorised access.
- (ix) ensure personnel not on the access list are properly escorted and supervised.
- (x) ensure a site access log is maintained at the Certifying Authority's operational site and inspected periodically.

(4) Multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup

capable of continuing operation even in the event of loss of main power. Electrical/Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.

- (5) Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinized and maintained for at least one year.
- (6) A Certifying Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Guidelines given at Schedule-II.
- (7) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.
- (8) Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorised personnel.
- (9) By-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.
- (10) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.
- (11) Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.
- (12) System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Guidelines given at Schedule-II.

4. Media Storage

A Certifying Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with para 8.3 and para 8.4 of the Information Technology Security Guidelines given at Schedule-II.

5. Waste Disposal

All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinized before being destroyed or released for disposal.

6. Off-site Backup

A Certifying Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certifying Authority site.

7. Change and Configuration Management

- (1) The components of the Certifying Authority infrastructure (e.g. cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security etc.) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.
- (2) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.
- (3) Software updates and patches shall be reviewed for security implications before being implemented on Certifying Authority's system.
- (4) Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented.

(5) Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented.

8. Network and Communications Security

- (1) Certifying Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Guidelines given at Schedule-II.
- (2) Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.
- (3) Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxy servers) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.
- (4) Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.
- (5) Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed.
- (6) Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

9. System Security Audit Procedures

9.1 Types of event recorded

(1) The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as:

- (i) System start-up and shutdown;
- (ii) Certifying Authority's application start-up and shutdown;
- (iii) Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
- (iv) Changes to keys of the Certifying Authority or any of his other details;
- (v) Changes to Digital Signature Certificate creation policies, e.g. validity period;
- (vi) Login and logoff attempts;
- (vii) Unauthorised attempts at network access to the Certifying Authority's system;
- (viii) Unauthorised attempts to access system files;
- (ix) Generation of own keys;
- (x) Creation and revocation of Digital Signature Certificates;
- (xi) Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys;
- (xii) Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

(2) Monitoring and Audit Logs

- (i) A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained:
 - (a) Registration;
 - (b) Certification;
 - (c) Publication;
 - (d) Suspension; and
 - (e) Revocation.

(ii) Records and log files shall be reviewed regularly for the following activities:

- (a) Misuse;
- (b) Errors;
- (c) Security violations;
- (d) Execution of privileged functions;
- (e) Change in access control lists;
- (f) Change in system configuration.

(3) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/subordinate/entity which caused the event.

(4) A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:

- (i) Physical access logs;
- (ii) System configuration changes and maintenance;
- (iii) Personnel changes;
- (iv) Discrepancy and compromise reports;
- (v) Records of the destruction of media containing key material, activation data, or personal subscriber information.

(5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be collected and consolidated, either electronically or manually, at a single location.

9.2 Frequency of Audit Log Monitoring

The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

9.3 Retention Period for Audit Log

The Certifying Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule-II.

9.4 Protection of Audit Log

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information must be protected from unauthorised viewing, modification and destruction.

9.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

9.6 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival

- (1) Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven years after the date of its expiration. This requirement does not include the backup of private signature keys.
- (2) Audit information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.
- (3) A second copy of all information retained or backed up must be stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such

as temperature, humidity and magnetism. The secondary site should be reachable in few hours.

- (4) All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properly constitutional warrant or such other legally enforceable document is produced.
- (5) The Certifying Authority should verify the integrity of the backups at least once every six months.
- (6) Information stored off-site must be periodically verified for data integrity.

11. Compromise and Disaster Recovery

11.1 Computing Resources, Software and/or Data are Corrupted

The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2 Secure facility after a natural or other type of disaster

The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3 Incident Management Plan

An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

- (i) Certifying Authority's certification key compromise;
- (ii) Hacking of systems and network;

- (iii) Breach of physical security;
- (iv) Infrastructure availability;
- (v) Fraudulent registration and generation of Digital Signature Certificates; and
- (vi) Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas:

- (i) Compromise control;
- (ii) Notification to user community; (if applicable)
- (iii) Revocation of affected Digital Signature Certificates; (if applicable)
- (iv) Responsibilities of personnel handling incidents;
- (v) Investigation of service disruption;
- (vi) Service restoration procedure;
- (vii) Monitoring and audit trail analysis; and
- (viii) Media and public relations.

12. Number of Persons Required Per Task

The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.

13. Identification and Authentication for Each Role

All Certifying Authority personnel must have their identity and authorization verified before they are:

- (i) included in the access list for the Certifying Authority's site;
- (ii) included in the access list for physical access to the Certifying Authority's system;

- (iii) given a certificate for the performance of their Certifying Authority role;
- (iv) given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certifying Authority's signing certificates) must:

- (i) be directly attributable to an individual;
- (ii) not be shared;
- (iii) be restricted to actions authorized for that role; and
- (iv) procedural controls.

Certifying Authority's operations must be secured using techniques of authentication and encryption, when accessed across-a shared network.

14. Personnel Security Controls

The Certifying Authority must ensure that all personnel performing duties with respect to its operation must:

- (i) be appointed in writing;
- (ii) be bound by contract or statute to the terms and conditions of the position they are to fill;
- (iii) have received comprehensive training with respect to the duties they are to perform;
- (iv) be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;
- (v) not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; and
- (vi) be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation.

15. Training Requirements

A Certifying Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in:

- (i) relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certifying Authority;

- (ii) all PKI software versions in use on the Certifying Authority's system;
- (iii) all PKI duties they are expected to perform; and
- (iv) disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirements

The requirements of para 15 must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel

A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

18. Key Management

18.1 Generation

- (1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.
- (2) The key generation process shall generate statistically random key values that are resistant to known attacks.

18.1 Distribution of Keys

Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

18.2 Storage

- (1) Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored

in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.

(2) The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and documented.

18.3 Usage

- (1) A system and software integrity check shall be performed prior to Certifying Authority's key loading.
- (2) Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control.

18.5 Certifying Authority's Public Key Delivery to Users

The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

19. Private Key Protection and Backup

- (1) The Certifying Authority must protect its private keys from disclosure.
- (2) The Certifying Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.
- (3) The Certifying Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

21. Usage Periods for the Public and Private Keys

21.1 Key Change

- (1) Certifying Authority and Subscriber keys shall be changed periodically.
- (2) Key change shall be processed as per Key Generation guidelines.
- (3) The Certifying Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.
- (4) The Certifying Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key.

All keys must have validity periods of no more than five years.

Suggested validity period:

- (a) Certifying Authority's root keys and associated certificates – five years;
- (b) Certifying Authority's private signing key - two years;
- (c) Subscriber Digital Signature Certificate key – three years;
- (d) Subscriber private key – three years.

Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

21.2 Destruction

Upon termination of use of a Certifying Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

21.3 Key Compromise

- (1) A procedure shall be pre-established to handle cases where a compromise of the Certifying Authority's Digital Signature private key has occurred. In such case, the Certifying Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.

- (2) The Certifying Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.
- (3) The Certifying Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.
- (4) Archives of Certifying Authority's public keys shall be protected from unauthorised modification.

22. Confidentiality of Subscriber's Information

- (1) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.
- (2) Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy.
- (3) A secure communication channel between the Certifying Authority and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

SCHEDULE-IV

[See rule 23]

Form for Application for issue of Digital Signature Certificate**For Individual/Hindu Undivided Family Applicant**

1. Full Name * [Name of the Karta in case of Hindu Undivided Family]

Last Name/Surname _____

First Name _____

Middle Name _____

2 Have you ever been known by any other name? If Yes,

Last Name/Surname _____

First Name _____

Middle Name _____

3. Address

*Residential Address **

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

State/Union Territory _____ Pin _____

Telephone No. _____

Fax _____

Mobile Phone No _____

*Office Address **

Name of Office _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____

State/Union Territory _____ Pin : _____

Telephone No. _____

Fax _____

4. Address for Communication * Tick \ as applicable A or B

5. Father's Name *

Last Name/Surname _____

First Name _____

Middle Name _____

6. Sex * (For Individual Applicant only) Tick \ as applicable : Male / Female

7. Date of Birth (dd/mm/yyyy) * ---/---/----

8. Nationality *

9. In case of foreign national, visa details _____

10. Credit Card Details

Credit Card Type _____

Credit Card No. _____

Issued By _____

11. E-mail Address _____

12. Web URL address _____

13. Passport Details #

Passport No. _____

Passport issuing authority _____

Passport expiry date _____

14. Voter's Identity Card No. # _____

15. Income Tax PAN no. # _____

16. ISP Details

ISP Name * _____

ISP's Website Address, if any _____

Your User Name at ISP, if any _____

17. Personal Web page URL, if any _____

For Company /Firm/Body of Individuals/Association of Persons/ Local Authority

18. Registration Number * _____

19. Date of Incorporation/Agreement/Partnership * ---/---/----

20. Particulars of Business, if any: *

Head Office _____

Name of Office _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____ Pin _____

State/Union Territory _____

Telephone No. _____

Fax _____

Web page URL, if any _____

No. of Branches _____

Nature of Business _____

21. Income Tax PAN No.* _____

22. Turnover in the last financial year Rs. _____

23 Names, Addresses etc. of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given below) *

Details of Partners/Members/Directors

No. of Partners/Members/Directors

Full Name

Last Name/Surname

First Name

Middle Name

Address

Flat/Door/Block No.

Name of Premises/Building/Village

Road/Street/Lane/Post Office

Area/Locality/Taluka/Sub-Division

Town/City/District

State/Union Territory Pin

Telephone No.

Fax No.

Mobile Phone No.

Nationality

In case of foreign national, Visa details

Passport Details #

Passport No.

Passport issuing authority

Passport expiry date

Voter's Identity Card No. #

Income Tax PAN no. #

E-mail Address

Personal Web page URL, if any

For Government Organisations/Agencies

24 Particulars of Organisation/Agency : *

Name of Organisation _____
 Administrative Ministry/Department _____
 Under State/Central Government _____
 Flat/Door/Block No. _____
 Name of Premises/Building/Village _____
 Road/Street/Lane/Post Office _____
 Area/Locality/Taluka/Sub-Division _____
 Town/City/District _____ Pin _____
 State/Union Territory _____
 Telephone No. _____
 Fax No. _____
 Name of the Head of Organisation _____
 Designation _____
 E-mail Address _____

25. Bank Details

Bank Name * _____
 Branch * _____
 Bank Account No. * _____
 Type of Bank Account * _____

26. Type of Digital Signature Certificate required *

27. Any other detail

Date

Signature of the Applicant

Instructions :

1. Columns marked with * are mandatory as applicable
2. For the columns marked with #, details for at least one is mandatory
3. Column No. 1 to 17 are to be filled up by individual applicants
4. Column No. 18 to 23 are to be filled up if applicant is a Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority.
5. Column No. 24 is to be filled up if applicant is a Government organization
6. Column No. 25 & 26 are to be filled up by all applicants.

SCHEDULE—V**Glossary****ACCEPT (A DIGITAL SIGNATURE CERTIFICATE)**

To demonstrate approval of a Digital Signature Certificate by a Digital Signature Certificate applicant while knowing or having notice of its informational contents

ACCESS

Gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network

ACCESS CONTROL

The process of limiting access to the resources of a computer system only to authorized users, programs or other computer systems

ACCREDITATION

A formal declaration by the Controller that a particular information system, professional or other employee or contractor, or organization is approved to perform certain duties and to operate in a specific security mode, using a prescribed set of safeguards

AUTHORITY REVOCATION LIST (ARL)

A list of revoked Certifying Authority certificates. An ARL is a CRL for Certifying Authority cross-certificates

ADDRESSEE

A person who is intended by the originator to receive the electronic record but does not include any intermediary

AFFILIATED CERTIFICATE

A certificate issued to an affiliated individual. (See also AFFILIATED INDIVIDUAL)

AFFIRM / AFFIRMATION

To state or indicate by conduct that data is correct or information is true

AFFIXING DIGITAL SIGNATURE

With its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

ALIAS

A pseudonym

APPLICANT (See CA APPLICANT, CERTIFICATE APPLICANT)**APPLICATION SOFTWARE**

A software that is specific to the solution of an application problem. It is the software coded by or for an end user that performs a service or relates to the user's work

APPLICATION SYSTEM

A family of products designed to offer solutions for commercial data processing, office and communications environments, as well as to provide simple, consistent programmer and end user interfaces for businesses of all sizes

ARCHIVE

To store records and associated journals for a given period of time for security, backup or auditing purposes

ASSURANCES

Statements or conduct intended to convey a general intention, supported by a good faith effort, to provide and maintain a specified service. "Assurances" does not necessarily imply a

guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties unless otherwise expressly indicated.

ASYMMETRIC CRYPTO SYSTEM

A system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

AUDIT

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUDIT TRAIL

A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

AUTHENTICATED RECORD

A signed document with appropriate assurances of authentication or a message with a digital signature verified by a relying party. However, for suspension and revocation notification purposes the digital signature contained in such notification message must have been created by the private key corresponding to the public key contained in the Digital Signature Certificate.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (See also VERIFY (a DIGITAL SIGNATURE))

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

BACKUP

The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

BINDING

An affirmation by a Certifying Authority of the relationship between a named entity and its public key.

CERTIFICATE

A Digital Signature Certificate issued by Certifying Authority.

CERTIFICATE CHAIN

An ordered list of certificates containing an end-user subscriber certificate and Certifying Authority certificates. (See VALID CERTIFICATE)

CERTIFICATE EXPIRATION

The time and date specified in the Digital Signature Certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION

An extension field to a Digital Signature Certificate which may convey additional information about the public key being certified, the certified subscriber, the Digital Signature Certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8 1995 (X.509). Custom extensions can also be defined by communities of interest.

CERTIFICATE ISSUANCE

The actions performed by a Certifying Authority in creating a Digital Signature Certificate and notifying the Digital Signature Certificate applicant (anticipated to become a subscriber) listed in the Digital Signature Certificate of its contents

CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]

Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital Signature Certificates. A Certifying Authority undertakes Digital Signature Certificate management functions by serving as a registration authority for subscriber Digital Signature Certificates. A Certifying Authority designates issued and accepted Digital Signature Certificates as valid by publication

CERTIFICATE POLICY

A specialized form of administrative policy tuned to electronic transactions performed during Digital Signature Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions such policies and associated enforcement technology can support provision of the security services required by particular applications

CERTIFICATE REVOCATION (SEE REVOKE A CERTIFICATE)**CERTIFICATE REVOCATION LIST (CRL)**

A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital Signature Certificates' serial numbers, and the specific times and reasons for suspension and revocation

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a Digital Signature Certificate generated by a Certifying Authority

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable form of a Digital Signature Certificate application

CERTIFICATE SUSPENSION (SEE SUSPEND A CERTIFICATE)**CERTIFICATION / CERTIFY**

The process of issuing a Digital Signature Certificate by a Certifying Authority

CERTIFYING AUTHORITY (CA)

A person who has been granted a licence to issue a Digital Signature Certificate under section 24 of Information Technology Act, 2000

CERTIFYING AUTHORITY SOFTWARE

The cryptographic software required to manage the keys of end entities

CERTIFYING AUTHORITY SYSTEM

All the hardware and software system (e.g. Computer, PKI servers, network devices etc) used by the Certifying Authority for generation, production, issue and management of Digital Signature Certificate

CERTIFICATION PRACTICE STATEMENT (CPS)

A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates

CERTIFIER (See ISSUING AUTHORITY)**CHALLENGE PHRASE**

A set of numbers and/or letters that are chosen by a Digital Signature Certificate applicant communicated to the Certifying Authority with a Digital Signature Certificate application and used by

the Certifying Authority to authenticate the subscriber for various purposes as required by the Certification Practice Statement. A challenge phrase is also used by a secret share holder to authenticate himself, herself, or itself to a secret share issuer

CERTIFICATE CLASS

A Digital Signature Certificate of a specified level of trust.

CLIENT APPLICATION

An application that runs on a personal computer or workstation and relies on a server to perform some operation

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, "common key" refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

COMMUNICATION/NETWORK SYSTEM

A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities (covering ISDN, lease lines, dial-up, LAN, WAN, etc.)

COMPROMISE

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over sensitive information may have occurred. (Cf. DATA INTEGRITY)

COMPUTER

Any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network

COMPUTER CENTRE (See DATA CENTRE)

COMPUTER DATA BASE

Means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

COMPUTER NETWORK

Interconnection of one or more computers through—

- (i) the use of satellite, microwave, terrestrial line or other communication media, and
- (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained

COMPUTER PERIPHERAL

Means equipment that works in conjunction with a computer but is not a part of the main computer itself, such as printer, magnetic tape reader, etc.

COMPUTER RESOURCE

Means computer, computer system, computer network, data, computer database or software

COMPUTER SYSTEM

A device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions

COMPUTER VIRUS (See VIRUS)

CONFIDENTIALITY

The condition in which sensitive data is kept secret and disclosed only to authorized parties

CONFIRM

To ascertain through appropriate inquiry and investigation (See also AUTHENTICATION VERIFY A DIGITAL SIGNATURE)

CONFIRMATION OF DIGITAL SIGNATURE CERTIFICATE CHAIN

The process of validating a Digital Signature Certificate chain and subsequently validating an end-user subscriber Digital Signature Certificate

CONTINGENCY PLANS

The establishment of emergency response, back up operation and post-disaster recovery processes maintained by an information processing facility or for an information system

Establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification and priority of what must be done who performs the required action, and what tools must be used.

A document, developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations such as disasters. Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

CONTROLS

Measures taken to ensure the integrity and quality of a process.

CORRESPOND

To belong to the same key pair (See also PUBLIC KEY, PRIVATE KEY)

CRITICAL INFORMATION

Data determined by the data owner as mission critical or essential to business purposes

CROSS-CERTIFICATE

A Certificate used to establish a trust relationship between two Certifying Authorities

CRYPTOGRAPHIC ALGORITHM

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

CRYPTOGRAPHY (See also PUBLIC KEY CRYPTOGRAPHY)

- (i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.
- (ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses

DAMAGE

Means to destroy, alter, delete, add, modify or rearrange any computer resource by any means

DATA

Means a representation of information knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

DATA BASE (See COMPUTER DATABASE)**DATA CENTRE (as also COMPUTER CENTRE)**

The facility covering the computer room, media library, network area, server area, programming and administration areas, other storage and support areas used to carry out the computer processing functions. Usually refers to the computer room and media library

DATA CONFIDENTIALITY (See CONFIDENTIALITY)

DATA INTEGRITY

A condition in which data has not been altered or destroyed in an unauthorized manner (See also THREAT, COMPROMISE)

DATA SECURITY

The practice of protecting data from accidental or malicious modification, destruction, or disclosure

DEMO CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority to be used exclusively for demonstration and presentation purposes and not for any secure or confidential communications. Demo Digital Signature Certificates may be used by authorized persons only

DIGITAL CERTIFICATE APPLICANT

A person that requests the issuance of a public key Digital Signature Certificate by a Certifying Authority. (See also CA APPLICANT; SUBSCRIBER)

DIGITAL CERTIFICATE APPLICATION

A request from a Digital Signature Certificate applicant (or authorized agent) to a Certifying Authority for the issuance of a Digital Signature Certificate (See also CERTIFICATE APPLICANT, CERTIFICATE SIGNING REQUEST)

DIGITAL SIGNATURE

Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.

DIGITAL SIGNATURE CERTIFICATE

Means a Digital Signature Certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context

DOCUMENT

A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information (See also MESSAGE; RECORD)

ELECTRONIC FORM

With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro-film, computer generated micro-fiche or similar device.

ELECTRONIC MAIL ("E-MAIL")

Messages sent, received or forwarded in digital form via a computer-based communication mechanism.

ELECTRONIC RECORD

Means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro-fiche.

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption)

EXTENSIONS

Extension fields in X 509 v3 certificates (See X 509)

FIREWALL/DOUBLE FIREWALL

One of several types of intelligent devices (such as routers or gateways) used to isolate networks. Firewalls make it difficult for attackers to jump from network to network. A double firewall is two firewalls connected together. Double firewalls are used to minimise risk if one firewall gets compromised or provide address translation functions.

FILE TRANSFER PROTOCOL (FTP)

The application protocol that offers file system access from the Internet suite of protocols

FUNCTION

In relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer

GATEWAY

Hardware or software that is used to translate protocols between two or more systems

GENERATE A KEY PAIR

A trustworthy process of creating private keys during Digital Signature Certificate's application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital Signature Certificate application in a manner that demonstrates the applicant's capacity to use the private key

HARD COPY

A copy of computer output that is printed on paper in a visually readable form e.g. printed reports, listing, and documents

HASH (HASH FUNCTION)

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that

- i) A message yields the same result every time the algorithm is executed using the same message as input.
- ii) It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm
- iii) It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm

HIGH-SECURITY ZONE

An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day a week by security staff, other personnel or electronic means.

IDENTIFICATION / IDENTIFY

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates

IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain

INFORMATION

Includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro fiche.

INFORMATION ASSETS

Means all information resources utilized in the course of any organisation's business and includes all information, application software (developed or purchased), and technology (hardware, system software and networks).

INTERMEDIARY

With respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message

INFORMATION TECHNOLOGY SECURITY

All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

INFORMATION TECHNOLOGY SECURITY POLICY

Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organization and its Information Technology systems

KEY

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation or signature verification).

KEY GENERATION

The trustworthy process of creating a private key/public key pair

KEY MANAGEMENT

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

KEY PAIR

In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key

LICENCE

Means a licence granted to a Certifying Authority

LOCAL AREA NETWORK (LAN)

A geographically small network of computers and supporting components used by a group or department to share related software and hardware resources

LOW-SENSITIVE

Applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure.

MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE [SEE CERTIFICATE MANAGEMENT]**MEDIA**

The material or configuration on which data is recorded. Examples include magnetic tapes and disks

MESSAGE

A digital representation of information; a computer-based record. A subset of RECORD (See also RECORD)

NAME

A set of identifying attributes purported to describe an entity of a certain type

NETWORK

A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities

NETWORK ADMINISTRATOR

The person at a computer network installation who designs, controls, and manages the use of the computer network

NODE

In a network, a point at which one or more functional units connect channels or data circuits

NOMINATED WEBSITE

A website designated by the Certifying Authority for display of information such as fee schedule, Certification Practice Statement, Certificate Policy etc.

NONREPUDIATION

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a digital signature verified pursuant to this Certification Practice Statement can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.

NOTARY

A natural person authorized by an executive governmental agency to perform notarial services such as taking acknowledgments, administering oaths or affirmations, witnessing or attesting signatures, and noting protests of negotiable instruments.

ON-LINE

Communications that provide a real-time connection.

OPERATIONS ZONE

An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

OPERATIONAL CERTIFICATE

A Digital Signature Certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

OPERATIONAL MANAGEMENT

Refers to all business/service unit management (i.e. the user management) as well as Information Technology management.

OPERATIONAL PERIOD

The period starting with the date and time a Digital Signature Certificate is issued (or on a later date and time certain if stated in the Digital Signature Certificate) and ending with the date and time on which the Digital Signature Certificate expires or is earlier suspended or revoked.

ORGANIZATION

An entity with which a user is affiliated. An organization may also be a user.

ORIGINATOR

A person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

PASSWORD (PASS PHRASE; PIN NUMBER)

Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.

PARTICULARLY SENSITIVE

Applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example loss of reputation or competitive advantage.

PC CARD (SEE ALSO SMART CARD)

A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON

Means any company or association or individual or body of individuals, whether incorporated or not.

PERSONAL PRESENCE

The act of appearing (physically rather than virtually or figuratively) before a Certifying Authority or its designee and proving one's identity as a prerequisite to Digital Signature Certificate issuance under certain circumstances.

PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER

A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital Signature Certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key certificates.

PKI HIERARCHY

A set of Certifying Authorities whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior Certifying Authority.

PLEDGE (See SOFTWARE PUBLISHER'S PLÉDGE)**POLICY**

A brief document that states the high-level organization position, states the scope, and establishes who is responsible for compliance with the policy and the corresponding standards. Following is an abbreviated example of what a policy may contain

- Introduction
- Definitions
- Policy Statement identifying the need for "something" (e.g. data security)
- Scope
- People playing a role and their responsibilities
- Statement of Enforcement, including responsibility

PRIVATE KEY

The key of a key pair used to create a digital signature.

PROCEDURE

A set of steps performed to ensure that a guideline is met.

PROGRAM

A detailed and explicit set of instructions for accomplishing some purpose, the set being expressed in some language suitable for input to a computer, or in machine language.

PROXY SERVER

A server that sits between a client application such as a web browser and a real server. It intercepts all requests to the real server to see if it can fulfill the request itself. If not, it forwards the request to the real server.

PUBLIC ACCESS ZONE

Generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorized activity.

PUBLIC KEY

The key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

PUBLIC KEY CERTIFICATE (See CERTIFICATE)**PUBLIC KEY CRYPTOGRAPHY (See CRYPTOGRAPHY)**

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations, used for the purpose of administering Digital Signature Certificates and keys.

PUBLIC/PRIVATE KEY PAIR (See PUBLIC KEY; PRIVATE KEY; KEY PAIR)**RECIPIENT (of a DIGITAL SIGNATURE)**

A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs. (See also RELYING PARTY)

RECORD

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term "record" is a superset of the two terms "document" and "message". (See also DOCUMENT; MESSAGE)

RE-ENROLLMENT (See also RENEWAL)**RELY / RELIANCE (on a CERTIFICATE and DIGITAL SIGNATURE)**

To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective. (See also RELYING PARTY; RECIPIENT)

RELYING PARTY

A recipient who acts in reliance on a certificate and digital signature (See also RECIPIENT, RELY OR RELIANCE (on a CERTIFICATE and DIGITAL SIGNATURE))

RENEWAL

The process of obtaining a new Digital Signature Certificate of the same class and type for the same subject once an existing Digital Signature Certificate has expired.

REPOSITORY

A database of Digital Signature Certificates and other relevant information accessible on-line

REPUDIATION (See also NONREPUDIATION)

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE

The process of permanently ending the operational period of a Digital Signature Certificate from a specified time forward.

RISK

The potential of damage to a system or associated assets that exists as a result of the combination of security threat and vulnerability.

RISK ANALYSIS

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

RISK ASSESSMENT

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

RISK MANAGEMENT

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect Information Technology system resources.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman.

SECRET SHARE

A portion of a cryptographic secret split among a number of physical tokens

SECRET SHARE HOLDER

An authorized holder of a physical token containing a secret share.

SECURE CHANNEL

A cryptographically enhanced communications path that protects messages against perceived security threats.

SECURE SYSTEM

Means computer hardware, software, and procedure that—
(a) are reasonably secure from unauthorised access and misuse.
(b) provide a reasonable level of reliability and correct operation,
(c) are reasonably suited to performing the intended functions, and
(d) adhere to generally accepted security procedures

SECURITY PROCEDURE

Means the security procedure prescribed under section 16 of the Information Technology Act, 2000

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations

SECURITY POLICY

A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system

SECURITY SERVICES

Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity

SECURITY ZONE

An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 weeks by security staff, other personnel or electronic means

SELF-SIGNED PUBLIC KEY

A data structure that is constructed the same as a Digital Signature Certificate but that is signed by its subject. Unlike a Digital Signature Certificate, a self-signed public key cannot be used in a trustworthy manner to authenticate a public key to other parties.

SERIAL NUMBER (See CERTIFICATE SERIAL NUMBER)**SERVER**

A computer system that responds to requests from client systems

SIGN

To create a digital signature for a message, or to affix a signature to a document, depending upon the context

SIGNATURE (See DIGITAL SIGNATURE)**SIGNER**

A person who creates a digital signature for a message, or a signature for a document

SMART CARD

A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME

A specification for E-mail security exploiting a cryptographic message syntax in an Internet MIME environment

SUBJECT (OF A CERTIFICATE)

The holder of a private key corresponding to a public key. The term "subject" can refer to both the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject's Digital Signature Certificate

SUBJECT NAME

The unambiguous value in the subject name field of a Digital Signature Certificate which is bound to the public key

SUBSCRIBER

A person in whose name the Digital Signature Certificate is issued

SUBSCRIBER AGREEMENT

The agreement executed between a subscriber and a Certifying Authority for the provision of designated public certification services in accordance with this Certification Practice Statement

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a Digital Signature Certificate application (*See also CERTIFICATE APPLICATION*)

SUSPEND A CERTIFICATE

A temporary "hold" placed on the effectiveness of the operational period of a Digital Signature Certificate without permanently revoking the Digital Signature Certificate. A Digital Signature Certificate suspension is invoked by, e.g., a CRL entry with a reason code (*See also REVOKE A CERTIFICATE*)

SYSTEM ADMINISTRATOR

The person at a computer installation who designs, controls, and manages the use of the computer system.

SYSTEM SECURITY

A system function that restricts the use of objects to certain users.

SYSTEM SOFTWARE

Application-independent software that supports the running of application software. It is a software that is part of or made available with a computer system and that determines how application programs are run; for example, an operating system.

TEST CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority for the limited purpose of internal technical testing. Test certificates may be used by authorized persons only.

THREAT

A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorized disclosure, or modification of data and/or denial of service

TIME-OUT

A security feature that logs off a user if any entry is not made at the terminal within a specified period of time

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

TOKEN

A hardware security token containing a user's private key(s), public key certificate, and optionally, a cache of other certificates, including all certificates in the user's certification chain

TRANSACTION

A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

TRUST

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certifying Authority. An authenticating entity must be certain that it can trust the Certifying Authority to create only valid and reliable Digital Signature Certificates, and users of those Digital Signature Certificates rely upon the authenticating entity's determination of trust.

TRUSTED POSITION

A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital Signature Certificates, including operations that restrict access to a repository.

TRUSTED THIRD PARTY

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (*Cf.*, TRUST)

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation, are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

TYPE (OF CERTIFICATE)

The defining properties of a Digital Signature Certificate, which limit its intended purpose to a class of applications uniquely, associated with that type.

UNAMBIGUOUS NAME (See DISTINGUISHED NAME)**UNIFORM RESOURCE LOCATOR (URL)**

A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

USER

An authorized entity that uses a certificate as applicant, subscriber, recipient or relying party, but not including the Certifying Authority issuing the Digital Signature Certificate. (See also CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER)

VALID CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority and accepted by the subscriber listed in it.

VALIDATE A CERTIFICATE (i.e., of an END-USER SUBSCRIBER CERTIFICATE)

The process performed by a recipient or relying party to confirm that an end-user subscriber Digital Signature Certificate is valid and was operational at the date and time a pertinent digital signature was created.

VALIDATION (OF CERTIFICATE APPLICATION)

The process performed by the Certifying Authority or its agent following submission of a Digital Signature Certificate application as a prerequisite to approval of the application and the issuance of a Digital Signature Certificate. (See also AUTHENTICATION; SOFTWARE VALIDATION)

VALIDATION (OF SOFTWARE) (See SOFTWARE VALIDATION)**VERIFY (A DIGITAL SIGNATURE)**

In relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether —

- (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
- (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

VIRUS

Means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

VULNERABILITY

A weakness that could be exploited to cause damage to the system or the assets it contains.

WEB BROWSER

A software application used to locate and display web pages

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

WRITING

Information in a record that is accessible and usable for subsequent reference.

X.509

The ITU-T (International Telecommunications Union-T) standard for Digital Signature Certificates. X 509 v3 refers to certificates containing or capable of containing extensions.

ACRONYMS

ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
e-mail	Electronic Mail
FTP	File Transfer Protocol
ISDN	Integrated Service Digital Network
ITU	International Telecommunications Union
LAN	Local Area Network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
URL	Uniform Resource Locator
WAN	Wide Area Network

अधिसूचना

नई दिल्ली, 17 अक्टूबर, 2000

सा.का.नि. 790(अ).—केंद्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 88 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, “साइबर विनियमन सलाहकार समिति” गठित करती है, जो निम्नलिखित से मिलकर बनेगी, अर्थात् :-

1. सूचना प्रौद्योगिकी मंत्री	अध्यक्ष
2. सचिव, विधायी विभाग	सदस्य
3. सचिव, सूचना प्रौद्योगिकी मंत्रालय	सदस्य
4. सचिव, दूरसंचार विभाग	सदस्य
5. सचिव, वित्त	सदस्य
6. सचिव, रक्षा मंत्रालय	सदस्य
7. सचिव, गृह मंत्रालय	सदस्य
8. सचिव, वाणिज्य मंत्रालय	सदस्य
9. उप गवर्नर, भारतीय रिजर्व बैंक	सदस्य
10. श्री टी. के. विश्वनाथन, संप्रति सदस्य सचिव, विधि आयोग	सदस्य
11. अध्यक्ष, नासकाम	सदस्य
12. अध्यक्ष, इंटरनेट सेवा प्रदाता संगम	सदस्य
13. निदेशक, केंद्रीय आसूचना ब्यूरो	सदस्य
14. नियंत्रक, प्रमाणन प्राधिकारी	सदस्य
15. राज्यों से चक्रानुक्रम द्वारा सूचना प्रौद्योगिकी सचिव	सदस्य
16. राज्यों से चक्रानुक्रम द्वारा पुलिस महानिदेशक	सदस्य
17. निदेशक, आई.आई.टी., चक्रानुक्रम द्वारा आई.आई.टी. से	सदस्य
18. सी.आई.आई. का प्रतिनिधि	सदस्य
19. एफ.वाई.सी.आई.आई. का प्रतिनिधि	सदस्य
20. एसोचैम का प्रतिनिधि	सदस्य
21. ज्येष्ठ निदेशक, सूचना प्रौद्योगिकी मंत्रालय	सदस्य
2. गैर शासकीय सदस्यों के लिए यात्रा भत्ता/महंगाई भत्ता, केंद्रीय सरकार के नियमों के अनुसार सूचना प्रौद्योगिकी मंत्रालय द्वारा वहन किया जाएगा ।	
3. समिति, विनिर्दिष्ट बैठकों के आधार पर, किसी व्यक्ति को सदस्य के रूप में सहयोगित कर सकेगी ।	

[सं. 1(20)/97-II डी (एन II)/एफ 6(iii)]

पी. एम. सिंह, संयुक्त सचिव

NOTIFICATION

New Delhi, the 17th October, 2000

G.S.R. 790(E).—In exercise of the powers conferred by section 88 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby constitute the “Cyber Regulation Advisory Committee”, consisting of the following, namely:—

1. Minister, Information Technology	Chairman
2. Secretary, Legislative Department	Member
3. Secretary, Ministry of Information Technology	Member
4. Secretary, Department of Telecommunications	Member
5. Finance Secretary	Member
6. Secretary, Ministry of Defence	Member
7. Secretary, Ministry of Home Affairs	Member
8. Secretary, Ministry of Commerce	Member
9. Deputy Governor, Reserve Bank of India	Member
10. Shri T K Vishwanathan, Presently Member Secretary, Law Commission	Member
11. President, NASSCOM	Member
12. President, Internet Service Providers Association	Member
13. Director, Central Bureau of Investigation	Member
14. Controller of Certifying Authority	Member
15. Information Technology Secretary by rotation from the States	Member
16. Director General of Police by rotation from the States	Member
17. Director, IIT by rotation from the IITs	Member
18. Representative of CII	Member
19. Representative of FICCI	Member
20. Representative of ASSOCHAM	Member
21. Senior Director, Ministry of Information Technology	Member Secretary

2. Travelling Allowance/Dearness Allowance, as per the Central Government rules, for the non-official members shall be borne by the Ministry of Information Technology.
3. The Committee may co-opt any person as member based on specific meetings.

[No. 1(20)/97-IID(NII)/F 6(iii)]

P. M. SINGH, Jt. Secy.

अधिसूचना

नई दिल्ली, 17 अक्टूबर, 2000

सा.का.नि. 791(अ).— केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, निम्नलिखित नियम बनाती है, अर्थात् :—

1. संक्षिप्त नाम और प्रारंभ— (1) इन नियमों का संक्षिप्त नाम साइबर विनियमन अपील अधिकरण (प्रक्रिया) नियम, 2000 है।

(2) ये राजपत्र में उनके प्रकाशन की तारीख को प्रवत्त होंगे।

2. परिभाषाएं— इन नियमों में, जक तक कि संदर्भ से अन्यथा अपेक्षित न हो,—

(क) “अधिनियम” से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) “अभिकर्ता” से किसी पक्षकार द्वारा अधिकरण के समक्ष इस निमित्त कोई आवेदन या उत्तर पेश करने के लिए सम्यक् रूप से प्राधिकृत कोई व्यक्ति अभिप्रेत है;

(ग) “आवेदन” से धारा 57 के अधीन अधिकरण को किया गया कोई आवेदन अभिप्रेत है;

(घ) “विधि व्यवसायी” का वही अर्थ होगा जो अधिवक्ता अधिनियम, 1961 (1961 का 25) में उसका है;

(ङ) “पीठासीन अधिकारी” से अधिकरण का पीठासीन अधिकारी अभिप्रेत है;

(च) “रजिस्ट्रार” से अधिकरण का रजिस्ट्रार अभिप्रेत है और कोई ऐसा अधिकारी भी है जिसको रजिस्ट्रार की शक्तियां और कृत्य प्रत्यायोजित किए जा सकेंगे;

(छ) “रजिस्ट्री” से अधिकरण की रजिस्ट्री अभिप्रेत है;

(ज) “धारा” से अधिनियम की धारा अभिप्रेत है;

(झ) “अंतरित आवेदन” से कोई वाद या अन्य कार्यवाही, जिसे धारा 29 की उपधारा (1) के अधीन अधिकरण को अंतरित किया गया है, अभिप्रेत है;

(झ) “अधिकरण” से धारा 48 के अधीन स्थापित साइबर विनियमन अपील अधिकरण अभिप्रेत है;

3. आवेदन फाइल करने की प्रक्रिया—(1) अधिकरण को कोई आवेदन, आवेदक द्वारा व्यक्तिगत रूप से या अभिकर्ता द्वारा या सम्यक् रूप से प्राधिकृत विधि व्यवसायी द्वारा इन नियमों में उपाबद्ध प्रलूप 1 में रजिस्ट्रार को प्रस्तुत किया जाएगा या रजिस्ट्रार को संबोधित करते हुए रजिस्ट्रीकृत डाक द्वारा भेजा जाएगा।

(2) उपनियम (1) के अधीन कोई आवेदन, प्रत्यर्थी के पूरे पते सहित फाइल आकार के एक खाली लिफाफे के साथ पेपर पुस्तिका के रूप में छह पूर्ण सेटों में प्रस्तुत किया जाएगा। जहां प्रत्यर्थियों की संख्या एक से अधिक है, वहां अतिरिक्त पेपर पुस्तिकाओं की पर्याप्त संख्या प्रत्येक प्रत्यर्थी के पुरे पते सहित फाहल आकार के खाली लिफाफों की अपेक्षित संख्यां के साथ, आवेदक द्वारा प्रस्तुत किए जाएंगे।

(3) आवेदक, अपने आवेदन के साथ प्रलूप-1 में दी गई प्राप्ति पर्ची संलग्न करके प्रस्तुत कर सकेगा जिस पूरे रजिस्ट्रार या रजिस्ट्रार की ओर से आवेदन प्राप्त करने वाला अधिकारी, आवेदन की प्राप्ति की पावती देगा।

(4) उपनियम (1), उपनियम (2) और उपनियम (3) में किसी बात के होते हुए भी, अधिकरण निम्नलिखित के बारे में अनुज्ञा दे सकेगा :-

(क) एक से अधिक व्यक्ति, संयुक्त रूप से एकल आवेदन फाइल कर सकेंगे यदि वाद हेतुक और प्रार्थित अनुतोष की प्रकृति को ध्यान में रखते हुए यह समाधान हो जाता है कि सेवा मामलों में उनके हित समान हैं।

(ख) एकल आवेदन में सम्मिलित होने के लिए इच्छुक व्यक्तियों का प्रतिनिधित्व कर रहा कोई संगम हो, तथापि, यह तब जब कि आवेदन में उन सभी व्यक्तियों के नाम प्रकट किए जाएंगे जिनकी ओर से यह फाइल किया गया है।

4. आवेदन का प्रस्तुतीकरण और संवीक्षा— (1) रजिस्ट्रार या रजिस्ट्रार द्वारा प्राधिकृत कोई अधिकारी प्रत्येक आवेदन पर वह तारीख पृष्ठांकित करेगा जिसको उस नियम के अधीन उसे प्रस्तुत किया गया या प्रस्तुत किया गया समझा जाएगा और वह पृष्ठांकन पर हस्ताक्षर करेगा।

(2) यदि, संवीक्षा करने पर आवेदन सुव्यवस्थित पाया जाता है तो इसे सम्यक् रूप से रजिस्ट्रीकृत किया जाएगा और क्रम संख्यांक दिया जाएगा।

(3) यदि संवीक्षा करने पर आवेदन त्रुटिपूर्ण पाया जाता है और देखी गई त्रुटि औपचारिक प्रकार की है तो रजिस्ट्रार अपनी उपस्थिति में पदभार को उसे सुधारने के लिए अनुज्ञा दे सकेगा और यदि उक्त त्रुटि औपचारिक प्रकार की नहीं है तो रजिस्ट्रार आवेदक को त्रुटि सुधारने के लिए ऐसा समय अनुज्ञात कर सकेगा जो वह ठीक समझे।

(4) यदि आवेदक, उपनियम (3) के अधीन अनुज्ञात समय के भीतर त्रुटि सुधारने में असफल रहता है तो रजिस्ट्रार ऐसे कारणों को लिखित रूप में अभिलिखित करते हुए आदेश द्वारा आवेदन कि रजिस्टर करने से इंकार कर सकेगा।

(5) उपनियम (4) के अधीन रजिस्ट्रार के आदेश के विरुद्ध कोई अपील ऐसा आदेश किए जाने के 15 दिन के भीतर अधिकरण को की जाएगी जिसका उस पर विनिश्चय अंतिम होगा।

5. आवेदन फाइल करने का स्थान— आवेदक रजिस्ट्रार के यहां आवेदन फाइल करेगा।

6. आवेदन की फीस— रजिस्ट्रार के यहां फाइल किए गए प्रत्येक आवेदन के साथ 2,000 रुपए केवल (दो हजार रुपए) की फीस, जो किसी अनुसूचित बैंक में रजिस्ट्रार के पक्ष में लिखे गए रेखांकित मांगदेय ड्राफ्ट या भुगतान आदेश के रूप में होगा और नई दिल्ली में संदेय होगा।

7. आवेदन की विषयवस्तु— (1) नियम 3 के अधीन फाइल किया गया प्रत्येक आवेदन सुमिन्नै शीर्षों के अधीन संक्षिप्त रूप से किया जाएगा। ऐसे आवेदन के लिए आधार और ऐसे आधार क्रमानुसार संख्यांकित किए जाएंगे और कागज के एक ओर दोहरे अंतर से टाइप किए जाएंगे।

(2) यदि आवेदन में आवेदन का अंतिम निपटान लंबित होने तक अंतरिम आदेश या निदेश के लिए प्रार्थना अंतर्निहित है तो अंतरिम आदेश या निर्देश प्राप्त करने के लिए पृथक् आवेदन करना आवश्यक नहीं होगा।

(3) अधिनियम की धारा 57 के अधीन आवेदन के फाइल करने के पश्चात् कोई आवेदक अंतरिम आदेश या निर्देश के लिए आवेदन कर सकेगा। ऐसा कोई आवेदन जहां तक संभव हो, उसी प्रलैप में होगा जो धारा 57 के अधीन विहित है, और उसके साथ 5 रुपए केवल (पांच रुपए) की फीस होगी जो ऐसे आवेदन पर लगी न्यायालय फीस स्टांप के रूप में संदेय होगी।

8. आवेदन के साथ पेपर-पुस्तिका आदि का होना— (1) प्रत्येक आवेदन के साथ पेपर-पुस्तिका जिसमें निम्नलिखित समाविष्ट होंगे :-

(i) उस आदेश की प्रमाणित प्रति जिसके विरुद्ध आवेदन फाइल किया गया है।

(ii) उन दस्तावेजों की प्रतियां जिन पर आवेदक द्वारा विश्वास किया गया है और जो आवेदन में निर्दिष्ट हैं, और

(iii) दस्तावेजों की अनुक्रमणिका ।

(2) उपनियम (1) में निर्दिष्ट दस्तावेजों को अधिवक्ता या राजपत्रित अधिकारी द्वारा अनुप्रमाणित किया जा सकेगा ।

(3) जहां आवेदन किसी अभिकर्ता द्वारा फाइल किया जाता है, वहां उसे ऐसे अभिकर्ता के रूप में कार्य करने के लिए प्राधिकृत करने वाले दस्तावेज भी आवेदन के साथ संलग्न होंगे :

परंतु जहां आवेदन किसी अधिवक्ता द्वारा फाइल किया जाता है वहां उसके साथ सम्यक् रूप से निष्पादित वकालतनामा होगा ।

9. एकाधिक उपचार— आवेदन एकल वाद हेतुक पर आधारित होगा और एक या अधिक अनुतोष चाहे जा सकेंगे परंतु यह तब जब कि वे एक दूसरे के पारिणामिक हों ।

10 प्रत्यर्थियों पर आवेदन की सूचना की तामील— (1) पेपस्स-पुस्तिका के रूप में आवेदन की एक साधारणतया रजिस्ट्रार द्वारा निम्नलिखित रीति में से किसी एक रीति द्वारा प्रत्येक प्रत्यर्थी पर तामील की जाएगी :-

(i) आवेदक के माध्यम से या प्रक्रिया तामीलकर्ता के माध्यम से दस्ती ;

(ii) पावती के साथ रजिस्ट्रीकृत डाक के माध्यम से ।

(2) उपनियम (1) में किसी बात के होते हुए भी रजिस्ट्रार प्रत्यर्थियों की संख्या और उनके निवास स्थान या कार्य और अन्य परिस्थितियों को ध्यान में रखते हुए निदेश दे सकेगा कि आवेदन की सूचना प्रत्यर्थी को किसी अन्य रीति से जिसमें प्रतिस्थापित तामील की कोई रीति भी है जो रजिस्ट्रार को ठीक और सुविधाजनक प्रतीत हो तामील की जाएगी ।

(3) प्रत्येक आवेदक, तामील या प्रक्रियाओं के निष्पादन के लिए किसी ऐसे आवेदन की बाबत जहां प्रत्यर्थियों की संख्या पांच से अधिक है, निम्नानुसार फीस का संदाय करेगा :-

(i) पांच प्रत्यर्थियों से अधिक प्रत्येक प्रत्यर्थी के लिए 50 रुपए (पचास रुपए) की राशि ; अथवा

(ii) जहां तामील ऐसी रीति में हो जिसे रजिस्ट्रार, उपनियम (2) के अधीन निदेश दे, वहां तामील किए जाने में उपगत वास्तविक प्रभार जो रजिस्ट्रार द्वारा अवधारित किए जा सकेंगे ।

(4) उपनियम (3) के अधीन तामील या प्रक्रियाओं के निष्पादन के लिए फीस, आवेदक द्वारा या तो रजिस्ट्रार के पक्ष में अनुसूचित बैंक में रेखांकित मांगदेय ड्राफ्ट के रूप में और उस केन्द्र में संदेय, जहां रजिस्ट्रार का कार्यालय स्थित है, भेजी जाएगी या रजिस्ट्रार के पक्ष में रेखांकित पोस्टल आर्डर के रूप में और उस केन्द्र के महा डाकघर में संदेय, जहां अधिकरण स्थित है, भेजी जाएगी ।

(5) उपनियम (1), उपनियम (2), उपनियम (3) और उपनियम (4) में किसी बात के होते हुए भी, यदि अधिकरण का यह समाधान हो जाता है कि सभी प्रत्यर्थियों पर आवेदन की सूचना तामील करना युक्तियुक्त रूप से व्यवहार्य नहीं है तो उसके लिए कारणों को लिखित में अभिलिखित करते हुए निदेश दे सकेगा कि इस बात के होते हुए भी कि कुछ प्रत्यर्थियों को आवेदन की सूचना की तामील नहीं हुई है, आवेदन पर सुनवाई होगी परंतु किसी आवेदन पर तब तक सुनवाई नहीं होगी जब तक :-

(i) यदि सरकार प्रत्यर्थी है तो सरकार को आवेदन की सूचना की तामील न कर दी गई हो ;

(ii) उस प्राधिकारी को आवेदन की सूचना की तामील न कर दी गई हो जिसने वह आदेश पारित किया है जिसके विरुद्ध आवेदन फाइल किया गया है ; और

(iii) अधिकरण का समाधान नहीं हो जाता है कि उन प्रत्यर्थियों जिनको आवेदन की सूचना की तामील नहीं हुओ हैं, के हित का भली प्रकार से और पर्याप्त रूप से उन प्रत्यर्थियों द्वारा प्रतिनिधित्व किया गया है जिन पर आवेदन की सूचना की तामील हुई है ।

11. प्रत्यर्थी द्वारा उत्तर और अन्य दस्तावेज फाइल किया जाना— (1) प्रत्यर्थी, उस पर आवेदन की सूचना की तामील की तारीख से एक मास के भीतर, रजिस्ट्रार को पेपर-पुस्तिका के रूप में, दस्तावेजों के साथ आवेदन का उत्तर छह पूर्ण सेटों में फाइल करेगा ।

(2) प्रत्यर्थी, आवेदक को या उसके अधिवक्ता को यदि कोई है उपनियम (1) में यथाउल्लिखित दस्तावेजों की प्रतियों सहित उत्तर की प्रति भी तामील करेगा और ऐसी तामीली का सबूत रजिस्ट्रार को फाइल करेगा । अधिकरण, प्रत्यर्थी द्वारा आवेदन करने पर, एक मास की अवधि की समाप्ति के पश्चात्, उत्तर फाइल करने की अनुज्ञा दे सकेगा ।

12. सुनवाई की तारीख और स्थान अधिसूचित किया जाए— अधिकरण, आवेदन की सुनवाई की तारीख और स्थान पक्षकारों को अधिसूचित करेगा ।

13. अधिकरण की बैठक— अधिकरण, साधारणतया अपनी बैठकें नई दिल्ली में करेगा :

परंतु यदि किसी समय अधिकरण के पीठासीन अधिकारी का यह समाधान हो जाता है कि ऐसी परिस्थितियां विद्यमान हैं जिनके कारण नई दिल्ली से भिन्न अन्य किसी स्थान में बैठक करना आवश्यक है तो पीठासीन अधिकारी किसी ऐसे समुचित स्थान पर बैठक करने का निर्देश दे सकेगा ।

14 आवेदनों पर विनिश्चय— (1) अधिकरण, अंतरित मामलों की सुनवाई का एक कलेंडर तैयार करेगा और जहां तक संभव हो कलेंडर के अनुसार मामलों की सुनवाई और विनिश्चय करेगा ।

(2) जहां तक संभव हो प्रत्येक आवेदन उसकी प्रस्तुतीकरण की तारीख के छह मास के भीतर सुना और विनिश्चित किया जाएगा ।

(3) उपनियम (1) और उपनियम (2) के प्रयोजनों के लिए अधिकरण को स्थगन से इंकार करने और मौखिक बहस के लिए समय सीमित करने की शक्ति होगी ।

15. आवेदक की चूक के लिए आवेदन पर कार्रवाई— (1) जहां आवेदन की सुनवाई के लिए नियत किसी तारीख पर या किसी अन्य ऐसी तारीख पर जिसको ऐसी सुनवाई स्थगित की जा सकेगी, जब आवेदक पर सुनवाई के लिए पुकार की जाए और आवेदक उपस्थित नहीं हो तो अधिकरण अपने विवेकानुसार या तो चूक के लिए आवेदन खारिज कर सकेगा या उसे सुन सकेगा और गुणागुण के आधार पर निर्णय कर सकेगा ।

(2) जहां आवेदन, चूक के लिए खारिज कर दिया गया हो और आवेदक बाद में उपसंजात होता है और अधिकरण का समाधान करता है कि उसके उपस्थित न होने का पर्याप्त कारण था जब आवेदन पर सुनवाई के लिए पुकारा गया था तब अधिकरण आवेदन खारिज करने का आदेश अपास्त करते हुए आदेश करेगा और उसे प्रत्यावर्तित करेगा ।

16. आवेदन पर एकपक्षीय सुनवाई— (1) जहां आवेदन की सुनवाई के लिए नियत तारीख पर या किसी अन्य तारीख पर जिसको ऐसी सुनवाई स्थगित की जा सकेगी, आवेदक उपस्थित होता है और प्रत्यर्थी उपस्थित नहीं होता है, जब आवेदन पर सुनवाई के लिए पुकार की जाए वहां अधिकरण अपने विवेकानुसार या तो उसे स्थगित कर सकेगा या सुनवाई करके आवेदन पर एकपक्षीय निर्णय दे सकेगा ।

(2) जहां किंसी आवेदन पर, प्रत्यर्थी या प्रत्यर्थियों के विरुद्ध एकपक्षीय सुनवाई हुई है वहां ऐसा प्रत्यर्थी या ऐसे प्रत्यर्थी अधिकरण को उस पर अपास्त आदेश के लिए आवेदन कर सकेंगे और यदि ऐसा प्रत्यर्थी या ऐसे प्रत्यर्थी अधिकरण का समाधान कर देते हैं कि सूचना की सम्यक् रूप से तामील नहीं हुई थी या उसे या उन्हें उपस्थित होने से किसी पर्याप्त कारण से रोका गया था जब सुनवाई के लिए आवेदन पर पुकार हुई थी, तब अधिकरण उसके या

उनके विरुद्ध ऐसे निबंधनों पर जो वह ठीक समझे, एकपक्षीय सुनवाई को अपास्त करने का आदेश कर सकेगा और आवेदन पर कार्यवाही के लिए कोई दिन नियत करेगा :

परंतु जहां आवेदन की एकपक्षीय सुनवाई ऐसे स्वरूप की है कि उसे केवल एक प्रत्यर्थी के विरुद्ध अपास्त नहीं किया जा सकता वहां वह सभी या उनमें के किसी प्रत्यर्थी के लिए भी अपास्त कर सकेगा :

परंतु यह और कि अधिकरण केवल इस आधार पर कि सूचना की तारीख में अनियमितता हुई है, किसी आवेदन की एकपक्षीय सुनवाई को अपास्त नहीं करेगा, यदि उसका यह समाधान हो जाता है कि प्रत्यर्थी के पास सुनवाई की तारीख की सूचना की और उपस्थित होने और आवेदक के दावे का उत्तर देने का पर्याप्त समय था ।

17. आवेदन का स्थगन— अधिकरण, ऐसे निबंधनों पर जो वह ठीक समझे कार्यवाही के किसी प्रक्रम पर आवेदन की सुनवाई को स्थगित कर सकेगा ।

18. आदेश का हस्ताक्षरित होना और उस पर तारीख डालना— अधिकरण का प्रत्येक आदेश लिखित रूप में होगा और पीठासीन अधिकारी द्वारा हस्ताक्षरित होगा और उस पर तारीख डाली जाएगी ।

19. आदेशों का प्रकाशन— अधिकरण के ऐसे आदेश जो किसी रिपोर्ट या प्रेस में प्रकाशन के लिए ठीक समझे जाएं, ऐसे निबंधनों और शर्तों पर जो अधिकरण अधिकथित करे, ऐसे प्रकाशन के लिए जारी कर सकेगा ।

20. पक्षकारों को आदेशों की संसूचना— किसी आवेदन पर पारित प्रत्येक आदेश आवेदक को या प्रत्यर्थी को व्यक्तिगत रूप में या निःशुल्क लागत पर रजिस्ट्रीकृत डाक से संसूचित किया जाएगा ।

21. अभिलेखों के निरीक्षण के लिए कोई फीस नहीं— आवेदन के किसी पक्षकार द्वारा लंबित आवेदन के अभिलेखों के निरीक्षण के लिए कोई फीस प्रभारित नहीं की जाएगी ।

22. कतिपय मामलों में आदेश और निदेश— अधिकरण ऐसे आदेश कर सकेगा या ऐसे निदेश दे सकेगा जो उसके आदेशों को प्रभावी करने के लिए या उसके संबंध में या उसकी कार्यवाही के दुरुपयोग को रोकने के लिए या न्याय के उद्देश्य को सुनिश्चित करने के लिए आवश्यक या समीचीन हों ।

23. विधि व्यवसायियों के लिपिकों का रजिस्ट्रीकरण— (1) किसी विधि व्यवसायी द्वारा नियोजित ऐसा लिपिक, जो उस अधिकरण, जिसमें विधि व्यवसायी साधारणतया व्यवसाय करता है, के अभिलेखों तक पहुंच रखने के लिए और इसके आदेशों की प्रतियां अभिप्राप्त करने के लिए उस रूप में अनुज्ञात है, “रजिस्ट्रीकृत लिपिक” के रूप में ज्ञात होगा ।

(2) कोई विधि व्यवसायी, जो अपने लिपिक को रजिस्ट्रीकृत कराने की वांछा रखता है, रजिस्ट्रार को प्ररूप-2 में एक आवेदन करेगा ।

(3) कोई विधि व्यवसायी एक समय में दो से अधिक रजिस्ट्रीकृत लिपिक तब तक नहीं रखेगा जब तक कि रजिस्ट्रार साधारण या विशेष आदेश द्वारा अन्यथा अनुज्ञात न करे ।

(4) सभी रजिस्ट्रीकृत लिपिकों का एक रजिस्टर रजिस्ट्रार के कार्यालय में रखा जाएगा और लिपिक के रजिस्ट्रीकरण के पश्चात्, रजिस्ट्रार उसके लिए एक पहचानपत्र जारी करने का निदेश देगा जो अहस्तांतरणीय होगा और जिस अधिकरण के किसी अधिकारी या किसी अन्य कर्मचारी द्वारा अनुरोध किए जाने पर धारक द्वारा प्रस्तुत किया जाएगा ।

(5) उपनियम (4) में उल्लिखित पहचानपत्र, अधिकरण के रजिस्ट्रार के हस्ताक्षर के अधीन जारी किया जाएगा ।

(6) जब कभी कोई विधि व्यवसायी किसी रजिस्ट्रीकृत लिपिक का नियोजन समाप्त कर देता है तो वह इस बात की जानकारी तुरंत एक पत्र के माध्यम से, जिसके साथ उसके लिपिक को जारी पहचानपत्र संलग्न होगा, रजिस्ट्रार को देगा और ऐसे पत्र की प्राप्ति पर उक्त रजिस्ट्रीकृत लिपिक का नाम रजिस्टर से हटा दिया जाएगा ।

24. अधिकरण का कार्य करने का समय— शनिवार, रविवार और अन्य अवकाश के दिनों के सिवाय, अधिकरण के कार्यालय, पीठासीन अधिकारी द्वारा किए गए किसी आदेश के अध्यधीन रहते हुए, प्रतिदिन 10.00 बजे पूर्वाह्न से 5.00 बजे अपराह्न तक खुले रहेंगे किंतु कोई कार्य, जब तक कि यह आवश्यक प्रकृति का न हो, किसी भी कार्य दिवस को 4.30 बजे अपराह्न के पश्चात् ग्रहण नहीं किया जाएगा ।

25. आधेकरण की बैठक का समय— अधिकरण की बैठक का समय साधारणतया अध्यक्ष द्वारा किए गए किसी आदेश के अधीन रहते हुए 10.30 बजे पूर्वाह्न से 1.00 बजे अपराह्न तक और 2.00 बजे अपराह्न से 5.00 बजे अपराह्न तक होगा ।

26. रजिस्ट्रार की शक्तियां और कृत्य— (1) रजिस्ट्रार अधिकरण के सभी अभिलेखों की अभिरक्षा रखेगा और ऐसे अन्य कृत्यों को करेगा जो उसे इन नियमों के अधीन या पीठासीन अधिकारी द्वारा समनुदेशित किए जाएं ।

(2) रजिस्ट्रार, पीठासीन अधिकारी के अनुमोदन से किन्हीं ऐसे कृत्यों को, जो रजिस्ट्रार द्वारा इन नियमों के अधीन किए जाने अपेक्षित हैं, अधिकरण के किसी अन्य अधिकारी को प्रत्यायोजित कर सकेगा ।

(3) रजिस्ट्रार की अनुपस्थिति में, पीठासीन अधिकारी द्वारा, उसकी ओर से लिखित में प्राधिकृत अधिकरण का कोई अधिकारी, रजिस्ट्रार के सभी या किसी कृत्य को कर सकेगा और सभी या किसी शक्ति का प्रयोग कर सकेगा ।

(4) रजिस्ट्रार, अधिकरण की शक्ति गुप्ता को आपनी अभिरक्षा में रखेगा ।

(5) रजिस्ट्रार, पीठासीन अधिकारी द्वारा दिए गए साधारण या विशेष निदेश के अधीन रहते हुए, अधिकरण की शासकीय मुद्रा को किसी आदेश, सूचना या अन्य आदेशिका पर लगाएगा ।

(6) रजिस्ट्रार को अधिकरण के किसी आदेश की प्रमाणित प्रति पर अधिकरण की मुद्रा लगाने को प्राधिकृत करने की लिखित में शक्ति होगी ।

27. रजिस्ट्रार की अतिरिक्त शक्तियां और कर्तव्य— इन नियमों में अन्यत्र प्रदत्त शक्तियों के अतिरिक्त रजिस्ट्रार की, पीठासीन अधिकारी के किसी साधारण या विशेष आदेश के अधीन रहते हुए, निम्नलिखित शक्तियां और कर्तव्य होंगे, अर्थात् :-

(i) सभी आवेदन और अन्य दस्तावेज, जिनके अंतर्गत अंतरित आवेदन भी हैं, प्राप्त करना ;

(ii) आवेदनों को रजिस्ट्रीकृत किए जाने से पूर्व, उनकी संवीक्षा के कारण उत्पन्न सभी प्रश्नों का विनिश्चय करना ;

(iii) अधिकरण को प्रस्तुत किसी आवेदन को अधिनियम और नियमों के अनुसार संशोधित किए जाने की अपेक्षा करना ;

(iv) अधिकरण के निदेशों के अधीन रहते हुए, आवेदनों या अन्य कार्यवाहियों की सुनवाई की तारीखें नियत करना और उनकी सूचनाए जारी करना ;

(v) अभिलेखों में कोई औपचारिक संशोधन करने का निदेश देना ;

(vi) कार्यवाहियों के पक्षकारों को दस्तावेजों की प्रतियां प्रदान करने का आदेश देना ;

(vii) अन्य आदेशिकाओं की सूचनाओं को तामील करने, नई सूचनाओं को जारी करने के लिए या उनका समय बढ़ाने के लिए आवेदनों से संबंधित सभी मामलों का निपटारा करना ;

(viii) किसी न्यायालय या अन्य प्राधिकारी की अभिरक्षा से अभिलेख की अध्यपेक्षा करना ;

(ix) आवेदन के लंबित रहने के दौरान, मृत पक्षकारों के विधिक प्रतिनिधियों के प्रतिस्थापन के लिए आवेदन प्राप्त करना और उनका निपटारा करना ;

(x) सिवाय उसके जहां प्रतिस्थापन में किसी आदेश को अपास्त करना या उसका उपशमन अंतर्वलित हो, वहां प्रतिस्थापन के लिए आवेदनों को प्राप्त करना और उनका निपटारा करना ; और

(xi) दस्तावेजों की वापसी के लिए पक्षकारों द्वारा किए गए आवेदनों को प्राप्त करना और उनका निपटारा करना ।

28. मुद्रा और संप्रतीक— अधिकरण की शासकीय मुद्रा और संप्रतीक वह होगी जो सरकार विनिर्दिष्ट करे ।

प्रस्तुति-1

(नियम 4 देखिए)

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 57 के अधीन आवेदन

अधिकरण के कार्यालय में प्रयोग के लिए

फाइल करने की तारीख

या

डाक द्वारा प्राप्त होने की तारीख

रजिस्ट्रीकरण संख्या

रजिस्ट्रार के हस्ताक्षर

साइबर विनियमन अपील अधिकरण के समक्ष

.....

.....

क	ख	आवेदक
	और	
ग	घ	प्रत्यर्थी

के बीच

आवेदन के बारे :

1. आवेदन की विशिष्टियां—

- (i) आवेदक का नाम
- (ii) पिता / पति का नाम
- (iii) पदनाम और वह कार्यालय जिसमें नियोजित है
- (iv) कार्यालय का पता
- (v) सभी सूचनाओं की तामील के लिए पता

2. प्रत्यर्थी की विशिष्टियां

- (i) प्रत्यर्थी का नाम और / या पदनाम
- (ii) प्रत्यर्थी का कार्यालय का पता
- (iii) सभी सूचनाओं की तामील के लिए पता

3. उस आदेश की विशिष्टयां जिसके विरुद्ध आवेदन किया गया है :-

आवेदन निम्नलिखित आदेश के विरुद्ध किया गया है -

- (i) आदेश संख्या
- (ii) तारीख
- (iii) द्वारा पारित
- (iv) विषय, संक्षेप में

4. अधिकरण की अधिकारिता :

आवेदक घोषणा करता है कि उस आदेश की जिसके विरुद्ध वह परिव्राण चाहता है, विषयवस्तु अधिकरण की अधिकारिता के भीतर है।

5. सीमा :

आवेदक यह और घोषणा करता है कि आवेदन सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 57 में विहित सीमा के भीतर है।

6. मामले के तथ्य :

मामले के तथ्य नीचे दिए गए हैं

(कालानुक्रम में तथ्यों का सक्षिप्त विवरण है, प्रत्येक पैरा में यथा सभव एक पृथक विवाद्यक, तथ्य अथवा अन्यथा अतिरिक्त हो)

7 मागा गया अनुतोष

ऊपर पैरा 6 में उल्लिखित तथ्यों को देखते हुए, आवेदक निम्नलिखित अनुतोष / अनुतोषों के लिए प्रार्थना करता है -

(नीचे मागा गया / मांगे गए अनुतोष / अनुतोषों को, ऐसे अनुतोष / अनुतोषों के आधार और विधिक उपबध (यदि कोई है) जिन पर विश्वास किया गया है, का विवरण देते हुए विनिर्दिष्ट करें) ।

8. अतिरिक्त आदेश यदि प्रार्थना की गई हो

आवेदन पर अतिरिक्त विनिश्चय लंबित रहते हुए, आवेदक निम्नलिखित अतिरिक्त आदेश जारी करने के लिए अनुरोध करता है -

(कारणों सहित प्रार्थना किए गए अतिरिक्त आदेश की प्रकृति का उल्लेख करें)

9. निःशोष किए गए उपचार / उपचारों के ब्यौरे

आवेदक घोषणा करता है कि उसने सुसंगत सेवा नियमों आदि के अधीन उसको उपलब्ध सभी उपचारों का उपयोग कर लिया है।

(यहा किए गए अभ्यावेदनों के और ऐसे अभ्यावेदन के परिणाम के ब्यौरे कालानुक्रम में हैं)

10. मामले का किसी अन्य न्यायालय आदि में लंबित न होना :

आवेदक यह घोषणा करता है कि वह मामला, जिसकी बाबत यह आवेदन किया गया है, किसी न्यायालय या किसी अन्य प्राधिकारी के समक्ष लंबित नहीं है अथवा उसे किसी न्यायालय या अन्य प्राधिकारी द्वारा खारिज नहीं किया गया है।

11. अनुक्रमणिका के ब्यौरे :

उन दस्तावेजों के, जिन पर विश्वास किया गया है, व्यौरों की अनुक्रमणिका, दो प्रतियों में संलग्न है ।

12. संलग्नकों की सूची :

सत्यापन

मैं, (आवेदक का नाम), जो का पुत्र/ की पुत्री / की पत्नी है, आयु है, के रूप में कार्यरत हूँ का निवासी / की निवासी हूँ सत्यापित करता हूँ / करती हूँ कि पैरा 1 से 13 तक की विषयवस्तु मेरी निजी जानकारी और विश्वास के अनुसार सही है और मैंने किसी सारांश तथ्य को छिपाया नहीं है ।

आवेदक के हस्ताक्षर

स्थान :

तारीख :

सेवा में,

रजिस्ट्रार,
साइबर विनियमन अपील अधिकरण,
नई दिल्ली

प्राप्ति पर्ची

श्री / श्रीमती जो कार्यालय में के रूप में कार्यरत है और के निवासी हैं, द्वारा साइबर विनियमन अपील अधिकरण में फाइल किए गए आवेदन की प्राप्ति स्वीकार की जाती है ।

प्रूल्प-2

(नियम 24 देखिए)

लिपिक के रजिस्ट्रीकरण के लिए आवेदन

1. उस विधि व्यवसायी का नाम जिसकी ओर से लिपिक का रजिस्ट्रीकरण किया जाना है ।
2. रजिस्ट्रीकरण किए जाने वाले लिपिक की विशिष्टियां—

- (i) पूरा नाम (स्पष्ट अक्षरों में)
- (ii) पिता का नाम
- (iii) आयु और जन्म की तारीख
- (iv) जन्म का स्थान
- (v) राष्ट्रियता
- (vi) शैक्षिक अर्हताएं
- (vii) पूर्व नियोजन की, यदि कोई है, विशिष्टियां

मैं (ऊपर नामित लिपिक) यह प्रतिज्ञान करता हूं कि मुझसे संबंधित विशिष्टियां सही हैं ।

3. क्या विधि व्यवसायी के पास उसके नियोजन में पहले से ही कोई रजिस्ट्रीकृत लिपिक है और क्या जिस लिपिक का रजिस्ट्रीकरण चाहा गया है वह पहले से ही रजिस्ट्रीकृत लिपिक के बदले में है या उसके अतिरिक्त है अथवा नहीं ।

4. क्या जिस लिपिक का रजिस्ट्रीकरण चाहा गया है वह पहले से ही किसी अन्य विधि व्यवसायी के लिपिक के रूप में रजिस्ट्रीकृत है और यदि ऐसा है तो ऐसे व्यवसायी का नाम ।

मैं (विधि व्यवसायी) प्रमाणित करता हूं कि ऊपर दी गई विशिष्टियां मेरी सर्वोत्तम जानकारी और विश्वास के अनुसार सही हैं और मुझे ऐसे किन्हीं तथ्यों का ज्ञान नहीं है तो उक्त (नाम) का लिपिक के रूप में रजिस्ट्रीकरण अवांछनीय बना देगा ।

तारीख

सेवा में,

रजिस्ट्रार,

..... अधिकरण ।

विधि व्यवसायी के हस्ताक्षर

NOTIFICATION

New Delhi, the 17th October, 2000

G.S.R. 791(E).—In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:—

1. **Short title and commencement.**— (1) These rules may be called the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000.
(2) They shall come into force on the date of publication in the Official Gazette.
2. **Definitions.**—In these rules, unless the context otherwise requires.—
 - (a) "Act" means the Information Technology Act, 2000; (21 of 2000);
 - (b) "agent" means a person duly authorised by a party to present an application or reply on its behalf before the Tribunal;
 - (c) "application" means an application made to the Tribunal under section 57;
 - (d) "legal practitioner" shall have the same meaning as is assigned to it in the Advocates Act, 1961 (25 of 1971);
 - (e) "Presiding Officer" means the Presiding Officer of the Tribunal;
 - (f) "Registrar" means the Registrar of the Tribunal and includes any officer to whom the powers and functions of the Registrar may be delegated;
 - (g) "registry" means the Registry of the Tribunal;
 - (h) "section" means a section of the Act;
 - (i) "transferred application" means the suit or other proceeding which has been transferred to the Tribunal under sub-section (1) of section 29;
 - (j) "Tribunal" means the Cyber Regulations Appellate Tribunal established under section 48.

3. Procedure for filing applications.- (1) An application to the Tribunal shall be presented in Form-1 annexed to these rules by the applicant in person or by an agent or by a duly authorized legal practitioner, to the Registrar or sent by registered post addressed to the Registrar.

(2) The application under sub-rule (1) shall be presented in six complete sets in a paper-book form along with one empty file size envelope bearing full address of the respondent. Where the number of respondents is more than one, sufficient number of extra paper-books together with required number of empty file size envelopes bearing the full address of each respondent shall be furnished by the applicant.

(3) The applicant may attach to and present with his application a receipt slips as in Form No. 1 which shall be signed by the Registrar or the officer receiving the applications on behalf of the Registrar in acknowledgement of the receipt of the application.

(4) Notwithstanding anything contained in sub rules (1), (2) and (3), the Tribunal may permit:—

(a) more than one person to join together and file a single application if it is satisfied, having regard to the cause of action and the nature of relief prayed for, that they have the same interest in the service matter; or

(b) an Association representing the persons desirous of joining in a single application provided, however, that the application shall disclose the names of all the persons on whose behalf it has been filed.

4. Presentation and scrutiny of applications.— (1) The Registrar, or the officer authorised by the Registrar shall endorse on every application the date on which it is presented or deemed to have been presented under that rule and shall sign the endorsement.

(2) If, on scrutiny, the application is found to be in order, it shall be duly registered and given a serial number.

(3) If the application, on scrutiny, is found to be defective, and the defect noticed is formal in nature, the Registrar may allow the party to rectify the same in his presence, and if the said defect is not formal in nature, the Registrar may allow the applicant such time to rectify the defect as he may deem fit.

(4) If the applicant fails to rectify the defect within the time allowed under sub rule (3), the Registrar may, by order and for reasons to be recorded in writing,

decline to register the application.

(5) An appeal against the order of the Registrar under sub rule (4) shall be made within 15 days of the making of such order to the Tribunal whose decision thereon shall be final.

5. Place of filing application.—The applicant shall file application with the Registrar.

6. Application fee.—Every application filed with the Registrar shall be accompanied by a fee of Rs. 2,000/- (rupees two thousand) only which shall be either in the form of a crossed demand draft or a pay order drawn on a Scheduled Bank in favour of the Registrar and payable at New Delhi.

7. Contents of application.—(1) Every application filed under rule 3 shall set forth concisely under distinct heads, the grounds for such application and such grounds shall be numbered consecutively and typed in double space on one side of the paper.

(2) It shall not be necessary to present a separate application to seek an interim order or direction if the application contains a prayer seeking an interim order or direction pending final disposal of the application.

(3) An application may, subsequent to the filing of application under section 57 of the Act, apply for an interim order or direction . Such an application shall, as far as possible, be in the same form as is prescribed for an application under section 57 and shall be accompanied by a fee of Rs. 5/- (Rupees five only) which shall be payable in court fee stamps affixed on such application.

8. Paper book, etc. to accompany the application.— (1) Every application shall be accompanied by a paper book containing:—

- (i) a certified copy of the order against which the application has been filed;
- (ii) copies of the documents relied upon by the applicant and referred to in the application; and
- (iii) an index of documents.

(2) The documents referred to in sub rule (1) may be attested by an advocate or by a Gazetted Officer.

(3) Where an Application is filed by an agent, documents authorising him to

act as such agent shall also be appended to the application :

Provided that where an application is filed by an advocate it shall be accompanied by a duly executed 'vakalatname'.

9. Plural remedies.—An application shall be based upon a single cause of action and may seek one or more reliefs provided they are consequential to one another.

10. Service of notice of application on the respondents.—(1) A copy of the application in the paper-book shall ordinarily be served on each of the respondents by the Registrar in one of the following modes:—

- (i) hand delivery (dasti) through the applicant or through a process server; or
- (ii) through registered post with acknowledgement due.

(2) Notwithstanding anything contained in sub rule (1), the Registrar may, taking into account the number of respondents and their places of residence or work and other circumstances direct that notice of the application shall be served upon the respondents in any other manner including any manner of substituted service, as it appear to the Registrar just and convenient.

(3) Every applicant shall pay a fee for the service or execution of processes, in respect of an application where the number of respondents exceeds five, as under:—

- (i) a sum of Rs. 50 (Rupees fifty) for each respondent in excess of five respondents; or
- (ii) where the service is in such manner as the Registrar may direct under sub rule (2), a sum not exceeding the actual charges incurred in effecting the service as may be determined by the Registrar.

(4) The fee for the service or execution of processes under 'sub rule (3) shall be remitted by the applicant either in the form of a crossed Demand Draft drawn on a Scheduled Bank in favour of the Registrar and payable at the station where Registrar's office is situated or remitted through a crossed Indian Postal Order drawn in favour of the Registrar and payable in General Post Office of the station where the Tribunal is located.

(5) Notwithstanding anything contained in sub rules (1), (2), (3) and (4), if the Tribunal is satisfied that it is not reasonably practicable to serve notice of application upon all the respondents, if may for reasons to be recorded in writing, direct that the application shall be heard notwithstanding that some of the respondents have not been served with notice of the application, provided that no application shall be heard unless:—

(i) notice of the application has been served on the Government, if Government is respondent;

(ii) notice of the application has been served on the authority which passed the order against which the application has been filed; and

(iii) the Tribunal is satisfied that the interests of the respondents on whom notice of the application has not been served are adequately and sufficiently represented by the respondents on whom notice of the application has been served.

11. Filing of reply and other documents by the respondent.—(1) The respondent shall file six complete sets containing the reply to the application alongwith the documents in a paper-book form with the Registrar within one month of the date of service of the notice of the application on him.

(2) The respondent shall also serve a copy of the reply along with copies of documents as mentioned in sub rule (1) to the applicant or his advocate, if any, and file proof of such service with the Registrar. The Tribunal may, on application by the respondent, allow filing of the reply after the expiry of the period of one month.

12. Date and place of hearing to be notified.—The Tribunal shall notify to the parties the date and the place of hearing of the application.

13. Sittings of the Tribunal.—The Tribunal shall ordinarily hold its sittings at New Delhi :

Provided that, if at any time, the Presiding Officer of the Tribunal is satisfied that circumstances exist which render it necessary to have sittings of the Tribunal at any place other than New Delhi the Presiding Officer may direct to hold the sittings at any such appropriate place.

14. **Decision on applications.**—(1) Tribunal shall draw up a calendar for the hearing of transferred cases and as far as possible hear and decide the cases according to the calendar.

(2) Every application shall be heard and decided, as far as possible, within six months of the date of its presentation.

(3) For purposes of sub-rule (1) and (2), the Tribunal shall have the power to decline an adjournment and to limit the time for oral arguments.

15. **Action on application for applicant's default.**—(1) Where on the date fixed for hearing of the application or on any other date to which such hearing may be adjourned, the applicant does not appear when the application is called on for hearing, the Tribunal may, in its discretion, either dismiss the application for default or hear and decide it on merit.

(2) Where an application has been dismissed for default and the applicant appears afterwards and satisfies the Tribunal that there was sufficient cause for his non-appearance when the application was called on for hearing, the Tribunal shall make an order setting aside the order dismissing the application and restore the same.

16. **Hearing on application ex parte.**—(1) Where on the date fixed for hearing the application or on any other date to which hearing is adjourned, the applicant appears and the respondent does not appear when the application is called on for hearing, the Tribunal may, in its discretion, adjourn or hear and decide the application *ex parte*.

(2) Where an application has been heard *ex parte* against a respondent or respondents, such respondent or respondents may apply to the Tribunal for an order to set it aside and if such respondent or respondents satisfy the Tribunal that the notice was not duly served, or that he or they were prevented by any sufficient cause from appearing when the application was called on for hearing, the Tribunal may make an order setting aside the *ex parte* hearing as against him or them upon such terms as it thinks fit, and shall appoint a day for proceeding with the application:

Provided that where the *ex parte* hearing of the application is of such nature that it cannot be set aside as against one respondent only, it may be set aside as against all or any of the other respondents also:

Provided further that Tribunal shall not set aside *ex parte* hearing of an

application merely on the ground that there has been an irregularity in the service of notice, if it is satisfied that the respondent had notice of the date of hearing and had sufficient time to appear and answer the applicant's claim.

17. Adjournment of application.—The Tribunal may on such terms as it deems fit and at any stage of the proceedings adjourn the hearing of the application.

18. Order to be signed and dated—Every order of the Tribunal shall be in writing and shall be signed and dated by the Presiding Officer.

19. Publication of orders.—Such of the orders of the Tribunal as are deemed fit for publication in any report or the press may be released for such publication on such terms and conditions as the Tribunal may lay down.

20. Communication of orders to parties.—Every order passed on an application shall be communicated to the applicant and to the respondent either in person or by registered post free of cost.

21. No fee for inspection of records.—No fee shall be charged for inspecting the records of a pending application by a party thereto.

22. Orders and directions in certain cases.—The Tribunal may make such orders or give such directions as may be necessary or expedient to give effect or in relation to its orders or to prevent abuse of its process or to secure the ends of justice.

23. Registration of legal practitioners clerks: —(1) A clerk employed by a legal practitioner and permitted as such to have access to the records and to obtain copies of the orders of the Tribunal in which the legal practitioner ordinarily practices shall be known as a "registered clerk".

(2) A legal practitioner desirous of registering his clerk shall make an application to the Registrar in Form 2.

(3) A legal practitioner shall have at a time not more than two registered clerks unless the Registrar by general or special order otherwise permits.

(4) A register of all the registered clerks shall, be maintained in the office of the Registrar and after registration of the clerk, the Registrar shall direct the issue of an identity card to him which shall be non transferable and shall be produced by the holder upon request by an officer or any other employee of the Tribunal.

(5) The identity card mentioned in sub-rule (4) shall be issued under the signatures of the Registrar of the Tribunal.

(6) whenever a legal practitioner ceases to employ a registered clerk, he shall notify the fact at once to the Registrar by means of a letter enclosing therewith the identity card issued to his clerk and on receipt of such letter the name of the said registered clerk shall be struck off from the register.

24. Working hours of the Tribunal— Except on Saturday, Sundays and other holidays, the offices of the Tribunal shall, subject to any order made by the Presiding Officer, remain open daily from 10.00 a.m. to 5.00 p.m. but no work, unless it is of an urgent nature, shall be admitted after 4.30 p.m. on any working day.

25. Sitting hours of the Tribunal,—The sitting hours of the Tribunal shall ordinarily be from 10.30 a.m. to 1.00 p.m. and 2.00 p.m. to 5.00 p.m. subject to any order made by the Chairman.

26. Powers and functions of the Registrar: —(1) The Register shall have the custody of the records of the Tribunal and shall exercise such other functions as may be assigned to him under these rules or by the Presiding Officer.

(2) The Registrar may, with the approval of the Presiding Officer, delegate to another officer of the Tribunal any functions required by these rules to be exercised by the Registrar.

(3) In the absence of the Registrar, officer of the Tribunal authorised in writing by the Presiding Officer in his behalf may perform or exercise all or any of the functions and powers of the Registrar.

(4) The Registrar shall keep in his custody the official seal of the Tribunal.

(5) The Registrar shall, subject to any general or special direction by the Presiding Officer, affix the official seal of the Tribunal on any order, notice or other process.

(6) The Registrar shall have the power to authorise in writing the affixing of the seal of the Tribunal on a certified copy of any order of the Tribunal.

27. Additional powers and duties of Registrar.— In addition to the powers conferred elsewhere in these rules, the Registrar shall have the following powers and duties subject to any general or special order of the Presiding Officer namely:—

- (i) to receive all applications and other documents including transferred applications;
- (ii) to decide all questions arising out of the scrutiny of the applications before they are registered;
- (iii) to require any application presented to the Tribunal to be amended in accordance with the Act and the rules;
- (iv) subject to the directions of the Tribunal (o fix dates of hearing of the applications or other proceedings and issue notices thereof ;
- (v) to direct any formal amendment of records;
- (vi) to order grant of copies of documents to parties to the proceedings;
- (vii) to dispose of all matters, relating to the service of notices of other processes, applications for the issue of fresh notices or for extending the time therefore;
- (viii) to requisition records from the custody of any court or other authority;
- (ix) to receive applications for the substitution of legal representatives of the deceased parties, during the pendency of the application;
- (x) to receive and dispose of applications for substitution, except where the substitution would involve setting aside an order or abatement; and
- (xi) to receive and dispose of application by parties for return of documents.

28. Seal and emblem—The official seal and emblem of the Tribunal shall be such as the Government may specify.

FORM-1

(See rule 4)

APPLICATION UNDER SECTION 57 OF THE INFORMATION TECHNOLOGY ACT, 2000

For use in Tribunal's Oflice

Date of Filing _____

OR

Date of Receipt By post _____

Registration No. _____

Signature of Registrar

IN THE CYBER REGULATIONS APPELLATE TRIBUNAL

BETWEEN**A** **B** **APPLICANT****AND****C** **D** **RESPONDENT****Details of Application :****1. Particulars of the applicant:—**

- (i) Name of the applicant
- (ii) Name of Father/Husband
- (iii) Designation and office in which employed
- (iv) Office Address
- (v) Address for service of all notice

2. Particulars of the respondent :

- (i) Name and/or designation of the respondent
- (ii) Office address of the respondent
- (iii) Address for service of all notices

3. Particulars of the Order against which application is made :

The application is against the following order:

- (i) Order No.
- (ii) Date
- (iii) Passed by
- (iv) Subject in brief

4. Jurisdiction of the Tribunal:

The applicant declares that the subject matter of the order against which he wants re-dressal is within the jurisdiction of the Tribunal.

5. Limitation.—

The applicant further declares that the application is within the limitation prescribed in section 57 of the Information Technology Act, 2000.

6. Fact of the case:—

The facts of the case are given below:—

(Give here a concise statement of facts in a chronological order, each paragraph containing as nearly as possible a separate issue, fact or otherwise).

7. Relief(s) sought :—

In view of the facts mentioned in para 6 above, the applicant prays for the following relief(s) :—

[Specify below the relief(s) sought explaining the ground for the relief(s) and the legal provisions (if any) relied upon].

8. Interim order, if prayed for :

Pending final decision on the application, the applicant seeks issue of the following interim order :—

(Give here the nature of the interim order prayed for with reasons).

9. Details of the remedies exhausted :—

The applicant declares that he has availed of all the remedies available to him under the relevant service rules, etc.

(Give here chronologically the details of representations made and the outcome of such representation).

10. Matter not pending with any other court, etc.—

The applicant further declares that the matter regarding which this application has been made is not pending before any court of law or any other authority or has not been rejected by any court of law or other authority.

11. Details of Index :—

An index in duplicate containing the details of the documents to be relied upon is enclosed.

12. List of enclosures :—

Verification :

I, _____ (name of the applicant),

S/o, D/o, W/o _____ age _____

working as _____ resident of _____

hereby verify that the contents from 1 to 13 are true to my personal knowledge and belief and that I have not suppressed any material facts.

Place :

Date :

Signature of applicant

To
 The Registrar,
 Cyber Regulation Appellate Tribunal
 New Delhi

RECEIPT SLIP

Receipt of the application filed in the Cyber Regulation Appellate Tribunal by
 Shri/Smt. _____ working as _____
 in the Office of _____ residing _____
 _____ acknowledged.

FORM - 2

(See Rule 24)

APPLICATION FOR THE REGISTRATION OF A CLERK

1. Name of legal practitioner on whose behalf the clerk is to be registered.
2. Particulars of the clerk to be registered.
 - (i) Full Name (in capitals)
 - (ii) Father's name
 - (iii) Age and date of birth
 - (iv) Place of birth
 - (v) Nationality
 - (vi) Educational qualifications
 - (vii) Particulars of previous employment, if any.

I, _____ (clerk above named) do hereby affirm that that the particulars relating to me are true.

3. Whether the legal practitioner has a clerk already registered in his employ and whether the clerk sought to be registered is in lieu of or in addition to the clerk already registered.
4. Whether the clerk sought to be registered is already registered as a clerk of any other legal practitioner and if so, the name of such practitioner.

I, _____ (legal practitioner) certify that the particulars given above are true to the best of my information and belief and that I am not aware of any facts which would render undesirable the registration of the said _____ (name) as a clerk.

Date:

Signature of legal practitioner

To

The Registrar of the Tribunal

[No. 1(20)/97-IID(NII)/F 6(iv)]

P. M. SINGH, Jt. Secy.